TAMPERE UNIVERSITY OF TECHNOLOGY

ANTERO SALOJÄRVI

DEPENDABILITY IN MOBILE GROUND ELECTRONICS

Master of Science Thesis

Examiners: PhD Matti Mäntysalo (TTY), DI Juha Koiranen (Vansco Electronics Oy)
Examiner and topic approved in the Faculty of Computing and Electrical engineering council meeting on 3rd of May 2010

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Electrical Engineering
SALOJÄRVI, ANTERO: Dependability in Mobile Ground Electronics
Master of Science Thesis, 63 pages, 5 Appendix pages
May 2010
Major: Electronics
Examiner: PhD Matti Mäntysalo
Keywords: Dependability, safety, reliability, machinery control, FMEDA, IEC 61508, ISO 25119, ISO 15998

Requirement for highly dependable machinery control system is growing from increased complexity of control systems and their ability to control critical machinery functions. This has been noticed by legal authorities and governing legislation is becoming effective. Legal requirements can be met by using methodology based on adequate functional safety standards. Standards require certain tools and methods for product life cycle planning and implementation. Development and operational work flow shall be adapted to fulfill those requirements. Main focus in the study is to interpret standard requirements to process changes and to understand basic philosophy for reliable programmable system hardware. Standards IEC 61508 and ISO 25119 are referenced as main source for requirements.

Dependability is based on failure avoidance and control. Study introduces several failure avoidance tools and methods. V-model based work flow is adapted to industry specific requirements. Model includes life cycle approach, deliverable list and assessment checklist for safety related project flow. Documentation structure for good traceability is introduced for unit specification. System level analysis is based on failure mode and effect studies and usage of fault tree modeling helps to understand links between events. Safety level targeting model based on risk graph is introduced for usage in machinery-control-systems. Usage of tools and methods was tested in machinery-control-system concept development. Developed concept is intended for operator interface and control tasks. Tools proved to be usable for engineering project and fully implemented documentation model shall fulfill basic assessment requirements. Developed concept itself is usable in critical control systems, but some fine tuning is needed.

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan koulutusohjelma
SALOJÄRVI, ANTERO: Käyttövarmuus liikkuvassa elektroniikassa
Diplomityö, 63 sivua, 5 liitesivua
Toukokuu 2010
Pääaine: Elektroniikka
Tarkastaja: PhD Matti Mäntysalo
Avainsanat: Käyttövarmuus, Turvallisuus, Luotettavuus, Koneenohjaus,
FMEDA, IEC 61508, ISO 25119, ISO 15998

Vaatimukset elektroniikan käyttövarmuudelle ovat kasvaneet viimeksi kuluneiden kymmenen vuoden aikana voimakkaasti, koska ohjausjärjestelmistä on tullut monimutkaisia ja ne ovat korvanneet mekaanisia turvalaitteita. Erityisesti turvallisuuskriittisten toimintojen ohjaaminen on yleistynyt. Muutos on huomattu myös tuoteturvallisuutta valvovien viranomaisten toimesta ja ohjausjärjestelmien toimintaa ja suunnittelua koskevia vaatimuksia on kehitetty. Lainsäädännölliset vaatimukset ovat tulossa voimaan lähiaikoina eri laiteympäristöille ja ne perustuvat olemassa oleviin toiminnallista turvallisuutta koskeviin standardeihin. Standardien mukaisuus savutetaan käyttämällä niissä kuvattuja toimintatapoja ja työkaluja koko tuotteen elinkaaren aikana aina esisuunnittelusta käytöstäpoistoon asti. Suunnittelu, kokoonpano ja asennustyön kulku tulee sovittaa täyttämään nuo vaatimukset. Työn tarkoituksena on selvittää keskeiset toimintatavat ja työkalut liittyen standardeihin ja käyttövarman elektroniikan toimintoihin. Toimintatapoja, työkaluja ja teknisiäratkaisuja arvioidaan myös työn aikana suunnitellun koneenohjauskonseptin kautta.

Käyttövarma koneenohajausjärjestelmä mahdollistaa laitteen luotettavan käytön vaarantamatta ihmisiä tai ympäristöä. Tärkeä osa käyttövarmuutta on myös käytön jatkuvuus ja huollettavuus suunnitellusti. Käyttövarmuus tuleekin nähdä tuotteeseen sisäänrakennettuna ominaisuutena suunnittelun, valmistuksen ja käytön aikana. Käyttövarmuus perustuu virhetilanteiden välttämiseen ja niiden vaikutusten kontrollointiin. Virheet voidaan jakaa kahteen päälohkoon. Satunnaisia virheitä esiintyy laitteen eliniän aikana, mutta niiden aiheuttamia vaikutuksia tulee kontrolloida ja pienentää suunnitellusti. Systemaattisia virheitä esiintyy järjestelmässä moninaisista syistä johtuen. Vaarallista vikaantumista voidaan välttää neljällä perustavalla. Laitteiston tulee vikaantua ennustettavalla tavalla. Laitteisto arkkitehtuurin valinnalla voidaan välttää turvallisuuden kannalta kriittisten pullonkaulojen muodostumista. Oikeita toimintapoja nuodattamalla voidaan vähentää systemaattisia virheitä laitteiston toteutuksessa. Standardit edellyttävät V-mallin mukaista toimintamallia tuotteen vaatimustenmukaisuuden varmistamiseksi. V-mallin rakenteen mukainen dokumentaatio tarjoaa jäljitettävyyden vaatimusten ja testauksen varmentamiseen.

Koneenohjauksessa tyypillinen konsepti on hajautettu järjestelmä, jossa usein käyttöliittymä ja varsinainen ohjaus on jaettu eri yksiköihin. Käyttöliittymäyksikkö on sijoitettu lähelle käyttäjää ja varsinainen ohjausyksikkö on kytketty käyttöliittymälaitteeseen sarjaliikenneliitynnällä. Turvallisuuden varmistamiseksi kommunikaatio on kahdennettu ja käytetty sarjaliikenneprotokolla noudattaa CAN standardia. CAN standardi tarjoaa itsessään hyvin virheensietokykyisen kommunikaation ja kahdennus varmistaa toiminnan fyysisten virheiden varalle. Käyttöliittymän tehtävänä on varmistaa oikeiden käskyjen välittäminen oikea-aikaisesti muulle ohjausjärjestelmälle käyttäjän niin halutessa. Ohjausyksiköt valvovat järjestelmän tilaa ja toimintaympäristöä ja tekevät päätöksen komennon toteuttamisesta turvallisuuden sallimissa rajoissa.

Järjestelmää analysoitiin ja määriteltiin turvallisuuden vaatimat eheystasot laitteiston toteutukselle. Tyypillisessä koneenohjausjärjestelmässä riskit liittyvät usein käyttäjän vaarantumiseen. Käyttäjää ja yksittäisiä sivullisia vaarantavan vikaantumiset vaativat jonkin verran keskimääräistä tasoa korkeampia turvallisuus eheystasoja. Tyypillisesti vaatimus on eheystaso kaksi. Konseptin vaatimustenmukaisuuden suunnitteluun ja varmistamiseen käytettiin lohkokaaviotasolla vikapuu-, vikamuoto- ja vaikutusanalyysejä. Komponenttitason vikamuoto-, vaikutus- ja kriittisyysanalyysillä (FMEDA) varmistettiin suunnitellun toteutuksen vaatimusten täyttymistä. Konseptin sinänsä havaittiin täyttävän perusvaatimukset hyvin, mutta tiettyjä yksityiskohtia erityisesti yksiköiden yhteisissä osissa tulee parantaa.

Järjestelmäsuunnitteluvaiheessa tulee käyttövarmuus asioita miettiä kokonaisuutena. Eri käyttövarmuus näkökohtien välillä syntyy ristiriitaisuuksia ja sovelluksen kannalta oikea katsantokanta kannattaa valita. Usein lainmukaisuus tulee varmistaa ja sen jälkeen kohdistaa suuntaus asiakasvaatimusten mukaan. Siirtyminen hallittuun turvakriittiseen järjestelmäsuunnitteluun on usein asennekysymys organisaatiotasolla ja teknisesti ottaen ratkaisut kannattaa pitää mahdollisimman yksinkertaisina!

FOREWORD

Work for this Master of Science Thesis has been made in Vansco Electronics Oy (Part of Parker Hannifin Oy) during years 2009 and 2010.

I would like to thank examiners of Master of Science Thesis PhD Matti Mäntysalo and MSc Juha Koiranen for patients and good advice during work. Also Mr. Ari Vuorinen deserves my warm thank you for possibility to work with electronics for high reliability applications during last decade and also for encouraging me to finally make my Master of Science Thesis.

My fellow engineers in Wärtsilä and Parker Vansco have provided nice and cozy environment to work with. They have also helped me to gain some dependability related experience. Thank you boys!

In the end I would like thank Kirsi and Sebastian for patients, love, and understanding!

Ylöjärvellä 19. toukokuuta 2010

Antero Salojärvi

INDEX

TERMS AND DEFINITIONS

t_{exp}	Exposure time for operator or bystander
t_{avop}	Average operating time
λ/λ_{TOT}	Total failure rate for function
λ_{SD}	Safe and detected failures
λ_{SU}	Safe and undetected failures
λ_{DD}	Dangerous and detected failures
λ_{DU}	Dangerous and undetected failures
SIL	Safety Integrity Level
SRL	Safety Requirement Level
SFF	Safety Failure Fraction
FMEA	Failure Mode and Effect Analysis
FMEDA	Failure Mode, Effect and Diagnostics Analysis
IEC	International Electro technical Commission
ISO	International Standardization Organization
CAN	Controller Area Network, Automotive
ECU	Electronic Control Unit
OEM	Original Equipment Manufacturer
AgPL	Agriculture Performance Level
PE-system /PES	Programmable Electronic System
FIT	Failure In Time, Unit 1/10^{-9} h
TFT	Thin Film Transistor, Active LCL display type
MTTF	Mean Time To Failure
MTBF	Mean Time Between Failure
HMI	Human Machine Interface
CPU	Central Processing Unit
UML	Unified Modeling Language
QM	Quality assurance Measures
QS	Quality system
UML	Unified Modeling Language
V-model	Development model based on Verification and Validation (V figure)

1. INTRODUCTION

Requirement for highly dependable machinery control system is growing from increased complexity of control systems and their ability to control critical machinery functions. This has been noticed by legal authorities and governing legislation is becoming effective. New machinery directive 2006/42/EC for EU addresses electronic control systems in machinery. [11] New machinery directive was supposed to be applicable from beginning of 2010, but it is postponed for two years according to Official Journal of European Union. [20] Industry specific guideline standards for electronic controls are under development and partly released already. IEC 61508 forms a baseline for industry specific standards. Industry specific standards ISO 25119 (Agriculture and forestry machines) and ISO 15998 (Construction equipment) give implementation guidelines for methods introduced in baseline standard. Tool and methods provided by ISO 25119 are used widely in this study, since they fit well to machinery control applications.

Legal requirements can be met by using methodology based on adequate functional safety standards. Standards require certain tools and methods for product life cycle planning and implementation. Development and operational work flow shall be adapted to fulfill those requirements. Main focus in the study is to interpret standard requirements to process changes and to understand basic philosophy for reliable programmable system hardware. Usage of tools and methods is tested and demonstrated with machinery-control-system concept development.

Dependable control system provides continuously correct service for customer without hazardous consequences to people or public. System should be also maintained and modified in controlled manor. Dependability should be seen as built in feature for product development, manufacturing and operation phases. Dependability is based on failure avoidance and control. Failures can be qualified to two groups. Firstly there are failures which occur randomly and consequences of those failures should be controlled and effects minimized. Second failure category is systematic failures arising from wide range of causes. Avoidance of failures can be divided to four basic categories. Random failures should be controlled in proper manner. System should fail predictably and as planned and hardware architecture should avoid bottlenecks in system. Systematic errors shall be avoided with proper work flow.

Development of a new system starts with high level analysis and is focused to find links and chains between causes, failures and consequences. Discovered risks shall be quantified on their potentiality to harm people or environment. There is always a probability of catastrophic consequences, but likelihood should be in tolerable region compared to every day risks. System level analysis is based on failure mode and effect studies and usage of fault tree modeling helps to understand links between events. Systems level phase sets goals for integrity targets realized with implemented system. During design and realizations phase of the product life cycle detailed analysis of implemented devices provide evidence of achieved integrity levels. Reliability oriented development process and proper work flow in every step of product lifecycle will lead to reduced number of systematic failures. V-model based development process is highly recommended to provide feedback between requirements and testing evidence. Structured work methods and specifications provide good traceability between requirements and testing.

Typical system concept for machinery control is distributed system. Human interface device is located near operator and control unit is connected with serial interface to it. Communication redundancy is needed and two separate CAN lines provide needed protection against communication errors. Human interface device verifies that correct command is transmitted to system and it was intended to be commanded. ECU shall monitor system stage and operational conditions and makes decision to implement command only when it is safe. Safety integrity targets were analyzed and set after system level analysis. Results from Fault tree and Failure mode, effect and criticality (FMEDA) analysis indicated that concept fulfills requirements quite well, but on detail level diagnostics should be improved especially on common parts. Focus of dependability should be considered in the beginning of each project, since there is some trade offs between different dependability attributes.

Study is focused to methods and concepts related to hardware dependability. Software is equally important part of development project, but methods for software dependability differs significantly from hardware methods and due to space and time limitations software is left outside of the study scope. Chapter 2 represents overall life cycle concept and basic terminology related to control systems in hazardous systems. Dependability and safety should be seen as product life cycle challenge instead of just engineering task. Life cycle is illustrated as a background information for deeper analyze of electronic unit development. Chapters 3 and 4 concentrate to theory and interpretation of safety standard requirements. Chapter 5 gives implementation examples of tools and methods to achieve related requirements. Chapters 6 and 7 illustrate usage of tools and analyze results from concept machinery control system.

Document is intended to serve as a handbook for engineers working with safety projects in Parker Vansco. Other goal was to starts analysis of safe distributed machinery control system concept. Material related to concept analysis could serve as a technical sales material for future projects. In the end my personal goal is to develop skills to be able make high quality engineering work efficiently and in that sense methodology described in study works for all kind of products!

2. DEPENDABLE CONTROL SYSTEMS

Control system main feature is ability to control, protect or monitor process or equipment based on information flowing in from system input. System consists normally from several parts and all parts must fulfill safety related requirements. [8] Safety system analysis includes sensors, actuators, interface devices and communication media as well as logic subsystems as in Figure 1. Quest for higher dependability can be started from design reliability analysis. Modern functional safety standards provide a good starting point. For example IEC 61508 addresses electrical, electronic, programmable electronic systems. [1]

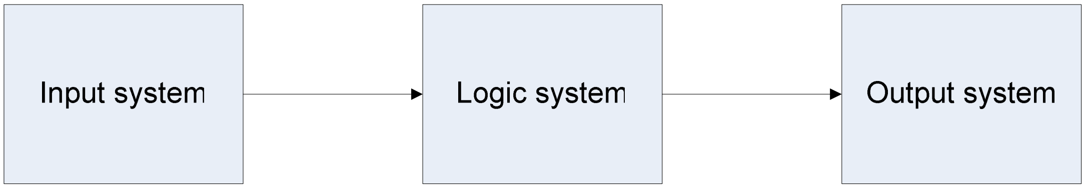


Figure 1 Basic electronic control system [8]

2.1. Dependability

Successful product development needs wider perspective than just safety legislation. Overall dependability on system level must be high to achieve high customer expectations. Safety is needed to be able to sell products, but dependability can be used as a sales argument. Dependability can be categorized as Figure 2.

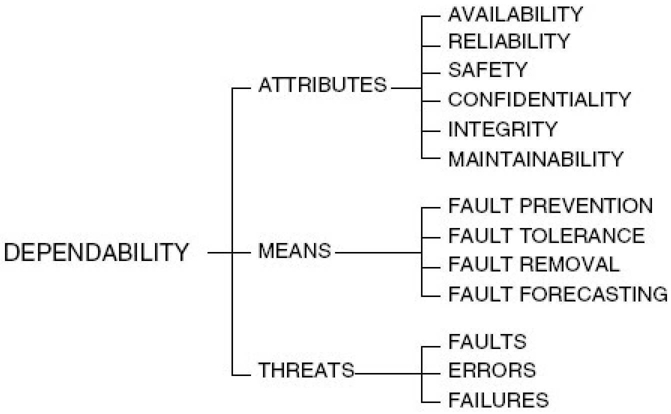


Figure 2 Concept of dependability according to Avizienis [6]

Attributes for dependability can be described as a collective term from availability, reliability, safety, integrity and maintainability. Definition of integrity includes also the term confidentiality in a sense of fail safe operation. Original equipment manufacturers (OEM) are responsible to system level reliability and safety. Suppliers mainly build devices and subsystems according specifications and targeted reliability and safety levels. Parker Vansco as a hardware supplier to OEM's takes responsibility of hardware subsystem or device realization phase. Study will be focused mainly to techniques and processes needed in that phase, although it is important to understand reliability and safety on the system level.

Widely accepted definitions for terms are as follows [2, 5, 6]:

> *"Availability - readiness for correct service"*
> *"Reliability - continuity of correct service"*
> *"Safety - absence of catastrophic consequences on the user(s) and the environment"*
> *"Integrity - absence of improper system alteration"*
> *"Maintainability - ability to undergo modifications and repairs" [15]*

In most cases availability, reliability and safety follow each other. Lately focus has been paid to safety aspects of control systems. Techniques adopted to safety analysis are actually used earlier in availability analysis. Safety aspects have brought more rigors to application of these techniques.[2] Study is concentrating to safety related system requirements, but same analysis address all five aspects of dependability. Focus of dependability should be considered in the beginning of each project, since there is some trade offs between different dependability attributes.

Means for improved dependability can be divided to three different areas. Three main areas cover whole life cycle of the product. In chronologic order they are design of system, manufacturing of system and operation of system. All three areas have different points of focus.

Design:

- Less complexity
- Redundancy where needed
- Stress factor overrating
- Testing of design and reviewing of design work
- Feedback based improvements during design iteration

Manufacturing:

- Control of materials, methods and changes
- Control of work methods and standards

Operation:

- Adequate user documentation
- Failure feedback from field
- Early involvement in systematic field failures

Threats for dependability are failures. They can be divided to two major categories. In all systems there is always risk of random events. Random failures cannot be prevented, but effects of random failures should be controlled on sufficient level. Second failure mode is systematic failures arising from life cycle activities. Systematic failures can be addressed with careful planning throughout design and operation. [2]

2.2. What is functional safety?

IEC 61508 defines safety as freedom from unacceptable risk of damage. Damage can be injury or threat to life. Also severe damages to environment and property must be considered as a safety issue. Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. [8] Functional safety can be described in other words as active safety. For example overall fire safety in house consists from several aspects. Brick walls are inherently safer than timber walls. Wall material is not anyway considered as functional safety. Installation of fire alarm devices to house can be seen as an improvement of functional safety, because fire alarm device reduces risks related to occupants. Also for example sprinkler systems would be considered as functional safety, since it has main task to limit damage to property. [1]

2.3. Cause, Failure, Consequence and Risk

To be able understand safety related analysis and mechanisms, one should consider difference in terms cause, failure, consequence and risk. Those terms are widely used in dependability and safety analysis. They form a chain of events in equipment under control and inside control system. [2]

Cause is the reason for failure in system. Causes can wary from environmental stresses to random effects in one component. Three main categories for causes are common causes like environmental stresses effecting whole system, systematic causes rising from engineering misunderstandings and random causes having impact only on certain parts of the system. [2]

Failures can be either physical or logical. They can be categorized as threats. Sometimes causes and failures are difficult to separate. For example in random component failure cause is random. In most cases probably some manufacturing and material tolerances are causing particular component to fail on specific time, but chain between specific cause and failure can be modeled only statistically. [2]

Consequence is what happens when failure occurs. When this consequence is directed to people, environment or property, it is often called as hazard. Consequence can be also another failure cause in the system. [2]

Risk is probability for realization of certain consequence. Risk is used in wider context as a total probability of hazardous consequences or as a probability to specific failure. Sometimes probability to specific failure can be called as occurrence. [2]

In most cases causes and consequences form chain reaction which will eventually lead to hazard. For example high ambient temperature may cause component failures in electronic modules. Component failures may lead to malfunction in operation. Malfunction in functional safety system is often hazardous. Functional safety systems often address those chain reactions and uses bypassing to avoid hazards. For example having two fire alarm devices in house is reducing risk of malfunction greatly! [1]

2.4. Tolerable risk

Functional safety standards start from the idea, that zero risk is unachievable. Also costs related to achieving lower risk levels tend to rise exponentially. Risks levels should be decreased to acceptable level to user and public. It is widely accepted that risk level for user can be higher than for the public. [2] IEC 61508 introduces safety integrity levels 1-4 with statistical risk levels introduced in Table 1. Risk levels refer to different levels of hazardous consequences to people. Levels 1-2 are mainly targeted for systems causing hazards to very few people and levels 3-4 are used in systems capable of harming multiple individuals. [8]

Table 1 Tolerable risk levels for systems causing possible hazard to people [8]

Safety integrity level (SIL)	High demand rate (Dangerous failures / hr)	Low demand rate (Probability of failure on demand)
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

Two columns are inherently the same. If failure in system (high demand) is once a year, figures end up to be equal. SIL level classification is based on failure potential to harm one or several people. For example nuclear power plant is allowed to plow up once in 100 000 years, since SIL4 is widely used in nuclear industry. On the other hand in construction machines only the user is exposed to hazard in most cases. Machine is also inherently quite safe due to safe cabins and slow speed. IEC 15998 indicate that in most cases SIL2 is adequate. [10] Statistically in worst case machine can fail hazardously once in 100 years in operation. Although there is no serious injury or death to people always related to failure. Let say that every tenth hazard causes serious injury and machine is operated 8 hours daily. Serious injury will happen in worst case once in 3000 years. 3,3 $*10^{-4}$ can be seen as a tolerable risk level for operator. In comparison Smith presents, that average risk for all deadly accidents in mid life is once in 5000 years. [1] Figures are rough ballpark values, but reason behind values in standard can be seen. In modern society smoking is considered as intolerable risk, but traffic is in tolerable region due to its benefits as in Figure 3. Risk for smoker to get deadly cancer is over one per mille in one year which is considered not worth of risk. Tolerable risk level for individual people is highly dependant from ideas and opinions. For example some people tend to think that risk from smoking is in tolerable region.

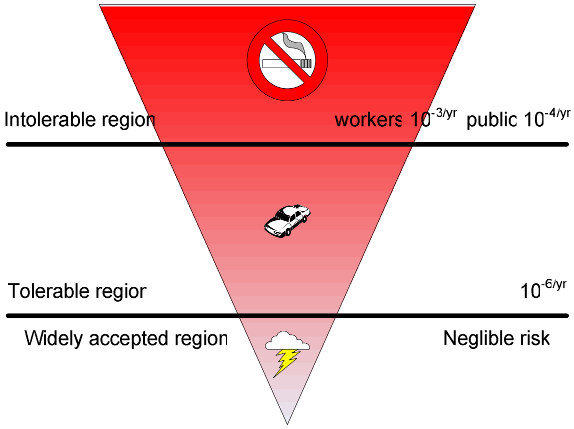


Figure 3 Tolerable risk level illustration

2.5. Product life cycle approach

According to IEC 61508 life cycle approach should be used in design and manufacturing of safety related systems [8]. Smith provides insight in to the life cycle model (Figure 4). Model should be adjusted to fulfill the needs of specific industry and company. Main idea behind life cycle approach is to record all events and failures during whole life cycle and react based on recorded data. [1]

In the Life cycle and System level scope phase high level safety plan shall be created. Main idea is to build up understanding of the system/equipment under control. Hazard identification should be made with proper techniques to discover all external and internal hazardous situations. [2]

System level risk analysis includes identification of hazards. Those shall be analyzed with relevant techniques to reveal potential risks to environment, users and public. Often failures cause multiple consequences and hazards. All risks are analyzed in quantified manner to be able to set risk levels. [2] During system level safety requirements and allocation maximum tolerable risk levels shall be set for the system. Overall safety integrity level will be assigned. All safety functions shall be identified and what failures are covered by those functions. All safety functions are classified to adequate safety integrity level. Safety system concept shall be created. [2]

System level planning should address whole life cycle of the product. Target is to guarantee safe operation in all life cycle phases. Plans should address also non technical issue like human errors and avoidance of those. It is important to understand what can be improved in the future and what lessons can be learned from the past experience. [2]

In the Unit design and Verification phase actual safety system or subsystems shall be designed, manufactured and build. Units shall be verified to fulfill all requirements related to safety and non-safety operation. Design phase should fulfill requirements set by related safety standard. Often phase can be seen as a project inside project and in some cases it can be a recursive project inside system level project. Especially custom made safety systems have their own life cycle inside system life cycle. Realization phase structure depends highly from industry and technological aspects. Most modern control systems include electronics and software running inside electronics. They are cross functional complex systems. [2] From that point of view V-model based design process is widely used and recognized by current standards. [9] In verification part subsystem or unit shall be tested to fulfill all safety and non safety functions. Verification should address all requirements and features and traceability must clear between specifications and test results. Structured documentation methods are a main method to demonstrate traceability requirements. [2]

System installation and integration phase includes build according to plans. Special attention should be paid on recording all events and especially failures. In case of serial productions, proper methods of pilot patch validation and field testing shall be applied. Also change management applies after start of production. [2] System validation shall be done according to validation plans. Validation should cover all aspects of the safety system. All test reports shall be reviewed and reviews documented. Revalidation should be carried out regularly to check recorded data during product life cycle. [2]

Operation, maintenance and modifications phase shall follow planned flow. Logs should be maintained and especially failures noted with adequate rigor. Modifications and redesign shall be made when necessary or safety targets are not achieved. Special attention shall be paid to field failure analysis. System documentation shall include maintenance schedule and instructions. Maintenance planning should be flexible and preventive maintenance is highly recommended. [2]

If decommissioning causes hazards to user, public or environment, those issues should be addressed in system safety planning. In many cases decommissioning can cause mainly possible environmental waste hazards, but also recycling should be planned for system life cycle. Quite often life time of subsystems is shorter than lifetime of the full system. Maintenance, modifications and decommissioning are more recursive than sequential phases in system life cycle model. In some cases decommissioning can be one of the most hazardous phases. For example in nuclear power plants decommissioning is major cost and risk. [1]

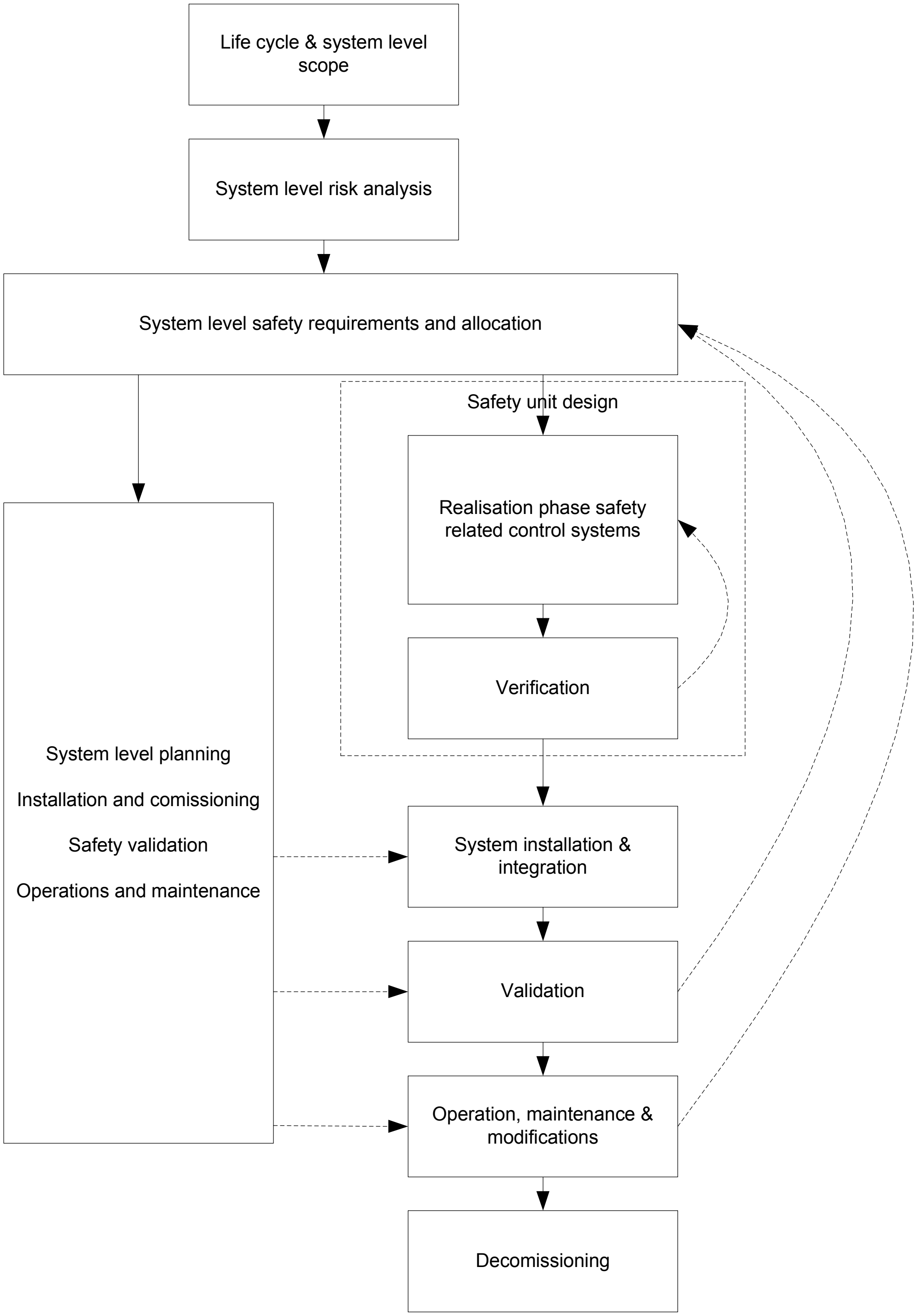

Life cycle & system level scope
System level risk analysis
System level safety requirements and allocation
Safety unit design
Realisation phase safety related control systems
Verification
System level planning
Installation and comissioning
Safety validation
Operations and maintenance
System installation & integration
Validation
Operation, maintenance & modifications
Decomissioning

Figure 4 Control system lifecycle [1]

Table 2 describes deliverables from different life cycle phases. These deliverables are highly recommended by safety standards. [1] During process audits and assessments deliverables are of the great interest.

Table 2 Deliverables from product life cycle [1]

Life cycle & System level scope
Safety plan Hazard identification documents
System level risk analyses
Risk analyses documents Safety concept including safety function descriptions Risk targets for system, subsystems and safety functions
System level planning
Installation instructions Validation plans User instructions Failure and operational log plans
Unit design and verification
Subsystem safety plan Structured product documents Pilot products Quantitative analyses of failure modes Verification plans Verification results
System installation and integration and validation
Installation logs Validation review documents Created event and modification logs for operation and maintenance phase
Operation, maintenance and modifications
Maintained event logs Maintained user manuals & maintenance instructions

3. RISK ASSESSMENT

Target of this paragraph is to provide general understanding of system level risk analysis. System level analysis shall be made by product OEM. Suppliers mainly need to fulfill requirements based on system level analysis. Risk assessment starts from target system analysis. When starting to think how requirements should be fulfilled in most rigorous way, causes for earlier faults should be analyzed. IEC16508 emphasizes lifecycle approach. Lessons learned from past shall be analyzed and results implemented to next generation systems. [8]

Typical error sources in complex system according to Smith:

- Random faults of hardware
- Faults in power supply system
- Environmental influences
- Human errors
- Systematic design flows
- Common cause failures
- Missing specification
- Wrong specification [1]

Figure 5 implicates, that major focus should be paid on specifications of any project phase. Also change management plays important role in avoidance of failures, although this study does not cover change management in detail. By knowing most error sources realization phase can be focused to avoid those errors, although as stated earlier zero failures is unrealistic goal.

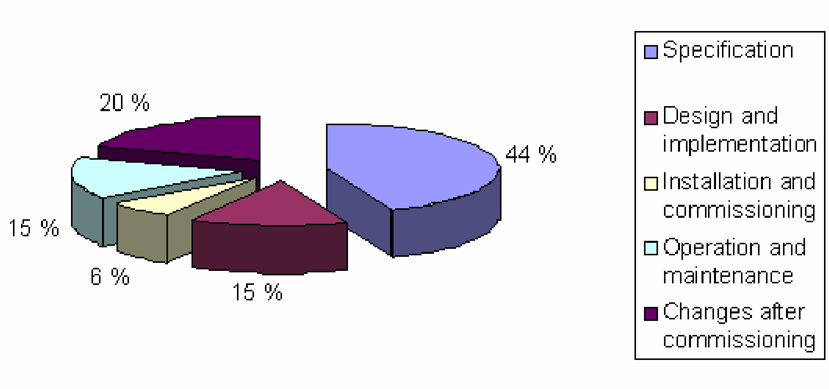


Figure 5 Primary causes for control system failures [4]

ISO 25199 describes workflow for risk analysis. First step is to have accurate system description and understanding of it. Next step is to discover surrounding conditions for target system. All operational states and conditions shall be derived from system descriptions. Preferred method is to make state flowcharts and transition tables. From this information a list of failures can be created. [9]

3.1. System failure analysis and integrity targets

Risk table approach can be used to analysis system failures as in Table 3. In risk table approach failures shall given classification according their severity, exposure and controllability. All listed failures shall be quantified according to all three main categories. Classification shall be documented as in Table 3.

Table 3 Failure classification table [9]

Failure	Severity	Exposure	Controllability
Failure 1	S2	E3	C3
Failure 2	S3	E2	C2
Failure N	S2	E3	C3

Severity analysis is focused to hazards directed to people. Severity classification should take operators and bystanders into account. Severity is based on most likely scenario and relevant operating conditions. Severity classification is divided to four categories based on potential harm to people as in Table 4:

Table 4 Failure severity classification [9]

S0	S1	S2	S3
No injuries	Light & moderate injuries	Severe & life threatening injuries	Fatal injuries

Exposure classification is based on probability of harmful failures implicating operator or bystander. Variable E is an estimation of how often or how long people are exposed to the hazard. Also the effect of operating conditions shall be taken into account. For example sliding on ice is only possible during winter. Five exposure categories quantify probability like in Table 5:

Table 5 Failure exposure classification [9]

E0	E1	E2	E3	E4
< 0,01%	0,1%	< 1%	< 10%	> 10%

Exposure can be expressed with following equation:

$$Exposure = \frac{t_{\exp}}{t_{avop}} \qquad \textbf{(1)}$$

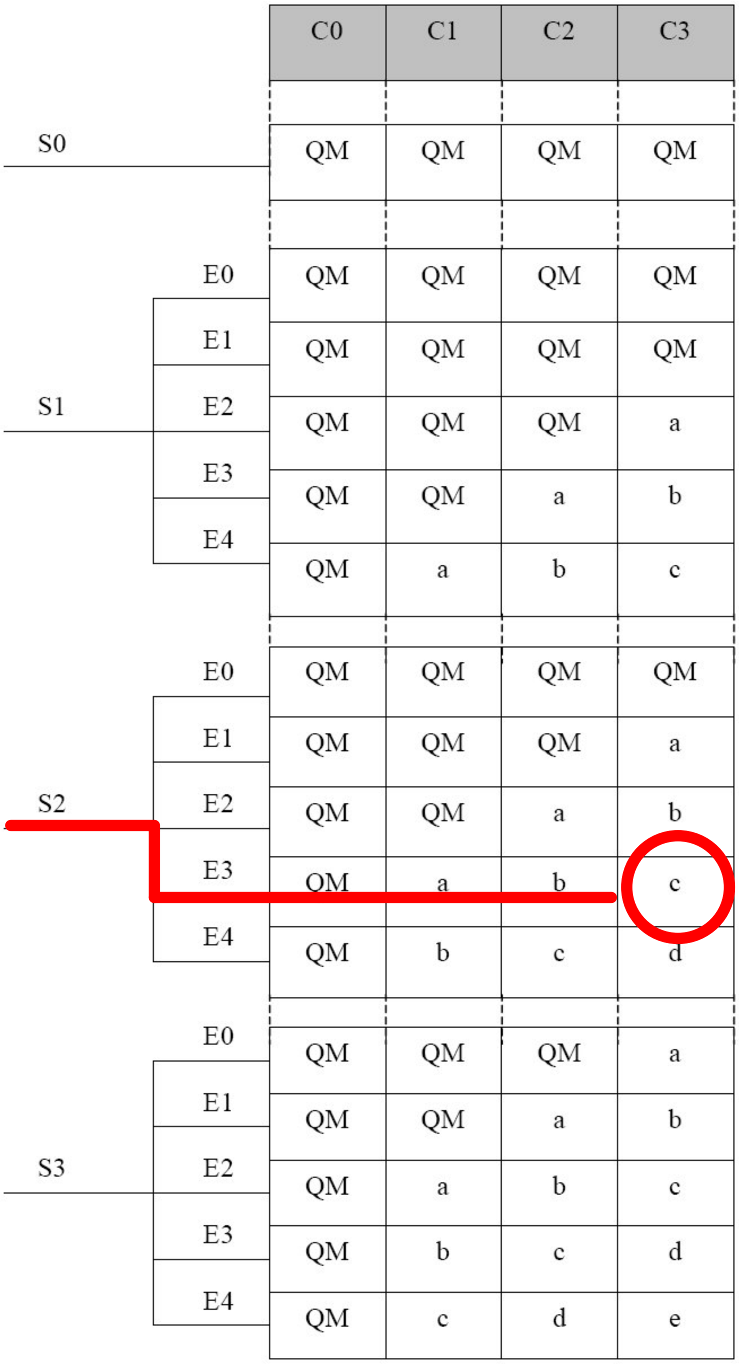
Where:
t_{exp} is exposure time by operator or bystander
t_{avop} is average operating time for function in question

Controllability is assessment of possible avoidance of harm by operator or bystander. If operator or bystander can easily prevent harmful situation, failure can be classifies as easily controllable. In the case of total loss of operator control or if failure cannot be noticed by operator or bystander failure it is classified as uncontrollable. For example jamming of gas pedal can be controlled easily by engine shutdown in vehicle. Four categories for controllability are as in Table 6.

Table 6 Failure controllability classification [9]

C0	C1	C2	C3
***Easily controllable*:** Operator or bystander can avoid harm with usual skills	***Controllable:*** The harm is almost always avoided , even for distracted operators or bystanders	***Generally controllable:*** Generally, the average operators or bystanders can avoid the harm	***Non controllable:*** The average operators or bystanders cannot generally avoid the harm

ISO 25119 presents risk graph approach as one method to evaluate needed safety integrity level from failure classification lists. For example failure 1 in Table 3 with severity level S2 starts from line S2. Exposure rating E3 leads to fourth line in S2 category. Failure has little controllability and therefore it goes to last column with C3 controllability rating. From Figure 6 can be read that safety integrity level required for particular failure is agriculture safety performance level (AgPL) c.



		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	QM	b	c	d
S3	E0	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	QM	b	c	d
	E4	QM	c	d	e

Figure 6 Selection table for agriculture equipment safety integrity level [9]

Key:
S = Severity,
E = Exposure to the hazardous event,
C = Controllability,
QM = Quality assurance measures,
a, b, c, d, e = Required Agricultural Performance Level ($AgPL_r$).

3.2. Selecting proper solution for implementation

System level planning is task for OEM, but suppliers should understand system also quite well to be able to make good solutions for implementation. Specification of system failures and operational modes gives good base for estimation requests or quotation. Selecting a proper implementation is then a task for supplier.

Selection of implementation needs two basic inputs:

- Overall safety integrity level requirement
- Safe state requirement

Table 7 sets requirement for hardware implementation based on AgPL level. Letter B and number from 1- to 3 describes required safety integrity level. Numbers are comparable to IEC 61508 SIL levels. [8] B stands for good engineering practice. Requirement in ISO 25119 is called software requirement level (SRL). Requirement refers to qualitative methods used in design. Mean time to fail (MTTF) set target for dangerous failure rates in one channel of system. Selection of higher reliability hardware architecture allows using lower level on systematic failure avoidance. [9] For example if one continues example with Table 3 failure 1, agriculture performance level c can be implemented with categories 1 to 4. By selecting category 2 software requirement level shall be 1, which is easier to achieve than level 2.

Table 7 ISO 25119 implementation selection table [9]

Agriculture performance level	CatB	Cat1	Cat2	Cat3	Cat4
a	1	B	B	B	B
b	2	1	B	B	B
c		2	1	1	1
d				2	2
e					3

	MTTF =	low	<30 000 FIT
░	MTTF =	medium	<10 000 FIT
▒	MTTF =	high	< 3 000 FIT

3.3. Risks assessment summary

After risk assessment requirements for hardware and software shall be documented. Hardware concept design starts from selected category solution and concept shall be described in detail. Testing and design documentation shall give evidence of requirement fulfillment.

According to ISO 25119 requirements for technical safety concept are:

- operational states
- safe states for all subsystems
- power up and down conditions including reset
- Reasonable unusual operational states
- Failure rates for channels and system
- Category requirements
- Failure diagnostic requirements according to category [9]

4. FOUR WAYS TO DECREASE RISK

Failure avoidance measures can be categorized to four sectors. Requirements are divided to qualitative and quantitative groups by their nature. Rigor of requirements differs between safety integrity levels, but main ideas are same. In this study focus is on SIL2 level requirements. All four parts in Figure 7 have equal weight. If any of the part of the puzzle is missing, product does not fulfill any safety integrity level.

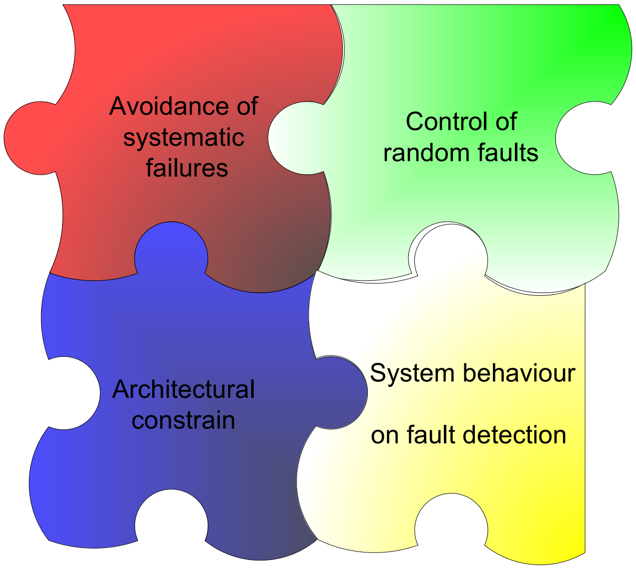

Avoidance of systematic failures
Control of random faults
Architectural constrain
System behaviour on fault detection

Figure 7 Four major requirements on way to improved safety

4.1.1. Qualitative requirements

Qualitative requirements address needs to avoid systematic failures. Systematic failures in IEC 61508 are addressed with two general requirements for all steps in development and design. Firstly all work must be planned and documented, secondly all work and documentation should be well structured and unambiguous. [8]

Avoiding systematic failure:

- Systematic and structural approach
- Verification step by step
- Planning and project management
- Good documentation in every step
- Good understanding from operational environment

Control of systematic failures:

- Control of operational environment
- Fault diagnostics in system
- Testing
    - EMC
    - Environmental stress testing
    - Destructive and over the limit testing

4.1.2. Design and development process features

ISO 25119 strongly suggest use of V-model based development work flow. [9] According to Haikala main benefits are minimized project risk, improved quality, reduction of life cycle cost and improved communication. Safety and reliability improvements are achieved mainly from improved quality and improved communication. Standardized development and strong structural approach make responsibilities more clear between project stakeholders. [3]

V-model emphasizes requirements driven process. Traceability must be seen as a two way street. (Figure 8) All requirements must be covered by at least one design element. Design elements must be linked to acceptance test. On the other hand all design elements must be based on at least one requirement. This ensures that implementation features are sufficient, but no extra features are included. Testing flow follows definition flow and requirements on certain level shall be verified on corresponding level. [9]

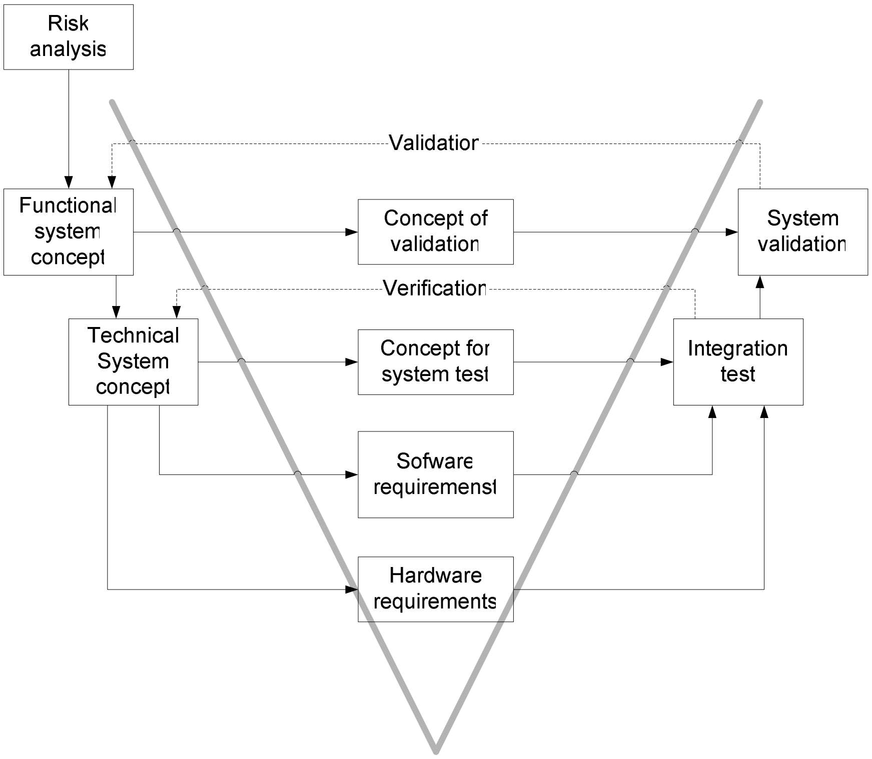


Figure 8 System design V-model [9]

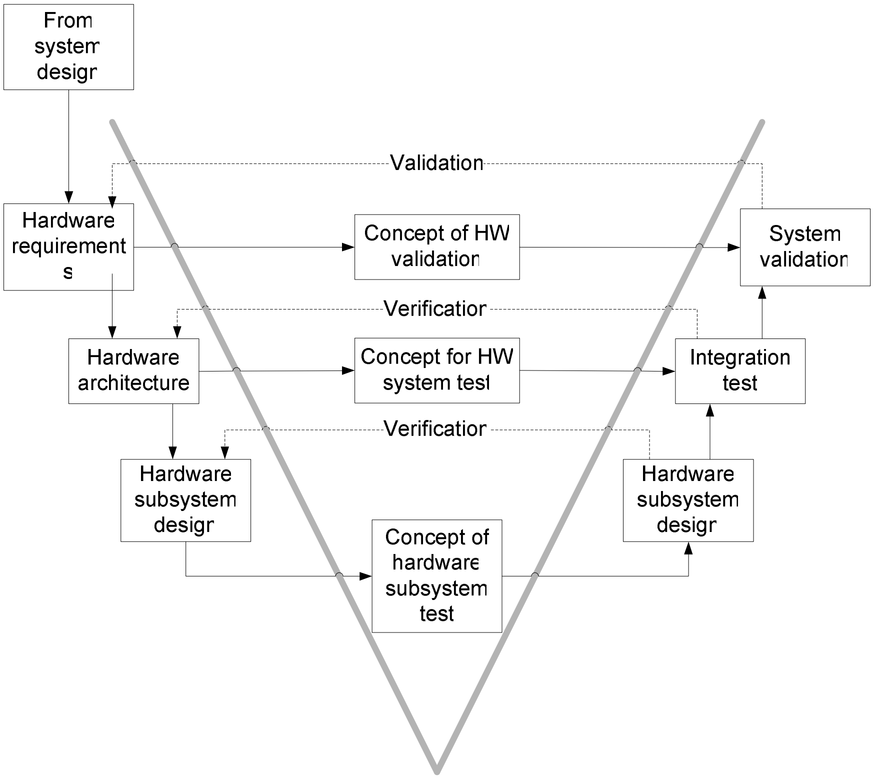


Figure 9 Hardware design V-model [9]

System design V-model divides to two parallel processes in realization phase. One side is for hardware design (Figure 9) and the other side for software. Two parallel processes have quite a lot cross-references and trade offs. Requirements between software and hardware section must be linked to each other. Figure 9 describes hardware design V-model. Software V-model is omitted, since it is quite similar and focus in study is in hardware requirements. [9]

4.1.3. Specifications

According to Smith specification should be well structured and structured design techniques implemented. Second requirement is unambiguousness of requirements. In modern control systems safety and control functions are often embedded to each other. Special attention should be paid to isolation between safety and non-safety functions. All data and electrical interfaces between safety systems and non-safety system should be tightly defined. If clear isolation is not possible, whole control system has to be safety critical. [1]

Main requirement for specification notation is to be clear, univocal and verifiable. For safety SIL 1 and 2 informal methods are adequate. In most cases natural language specification is used with explanatory support from semiformal modeling techniques. Attention should be paid to achieve adequate unambiguousness when using natural language. Semiformal methods are preferred for example by IEC61508. [8]

Logic diagrams, data dictionaries, data flow diagrams and truth tables are examples of semi formal methods suitable for specifications. [3]

ISO 25119 gives guidelines for documentation. Documentation follows closely structured design model. Specification model emphasizes linking of test cases to appropriate level requirements. Also tracking between subsequent specification levels is important. [9] Requirement specifications implicate **what** shall be implemented. Technical concept specifies **how** hardware implementation will fulfill higher level requirements.

Coverage for safety specification:

- Safety integrity level requirement
- Safety function requirements
- Safety system architecture
- Operating modes and performance
- External interface description
- Environmental requirements

According to Haikala specification phase is most important part of the project, since specification mistakes are hard to discover and they tend to be costly. Ideal specification has full coverage, high accuracy, total unambiguousness, testability and tracking without any mistakes. I real life ideal specification is impossible, because some requirements above have contrary effects. [3]

4.2. Quantitative analyze of random failures

Hardware random faults should be analyzed on detailed level. Proper documentation includes evidence from random failure calculations and analysis coverage. Statistical analyze is based on reliability data of each component and in most cases single failures will be covered. Single failure leading to other one is calculated as single failure. Two simultaneous non-connected failures are calculated as unlikely. Failure Modes Effects and Diagnostics Analysis (FMEDA) address failure rate and diagnostic coverage requirements. [2]

Control of random faults calls for three basic requirements [8]:

- Dangerous failure rate less than specified for particular integrity level.
- Safe failure fraction better than required for particular integrity level.
- Common cause failure control.

4.2.1. Failure rate

Failure rates can be calculated for subsystems and blocks as in Figure 10 and then combined for different safety channels. During the concept stage failure rates can be estimated for blocks and overall failure rate estimates can be made to verify concept. Also individual targets for realized blocks shall be set for detailed design. After detailed design failure rate verification can be done on component level. [2]

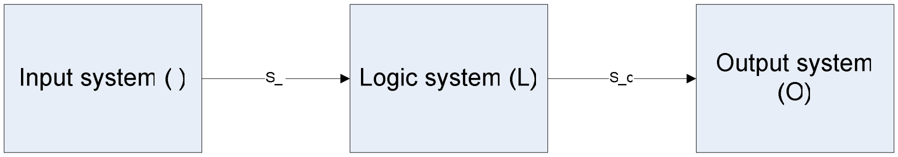


Figure 10 Basic PE-system

PE-system failure rate:

$$\lambda_{TOT} = \lambda_I + \lambda_L + \lambda_O \qquad \textbf{(2)}$$

Where:

λ is failure rate per time unit

Used units are [1/h] or more often [FIT] (1 FIT = 10^{-9}/h). Also Mean Time to Failure (MTTF) is used. MTTF is reciprocal value of the failure rate λ. Failure rate is easier to use in calculations, since values can be simply added together to calculate system failure rate. [2]

$$MTTF = \frac{1}{\lambda} \qquad \textbf{(3)}$$

4.2.2. Safe failure fraction

There is two simple ways to improve failure behavior of system. Design should be made in a way that most failures lead to safe state on system level. Secondly fast detection of failures and proper reaction to them is critical. According to IEC 61508 dangerous failure rate is critical factor. Failure classification divided to two issues. If failure is causing system level safety hazard, it is counted as dangerous failure. Otherwise failures are safe ones. If failure can be detected, it is detectable. Rest of failures is marked undetectable. In the end only dangerous undetected failures are really dangerous, if system can be put to safe state after failure detection without hazard to user or public (Figure 11).

Overall failure rate:

$$\lambda_{TOT} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU} \qquad \textbf{(4)}$$

Where:

λ_{SD} is safe and detected failures
λ_{SU} is safe and undetected failures
λ_{DD} is dangerous and detected failures
λ_{DU} is dangerous and undetected failures

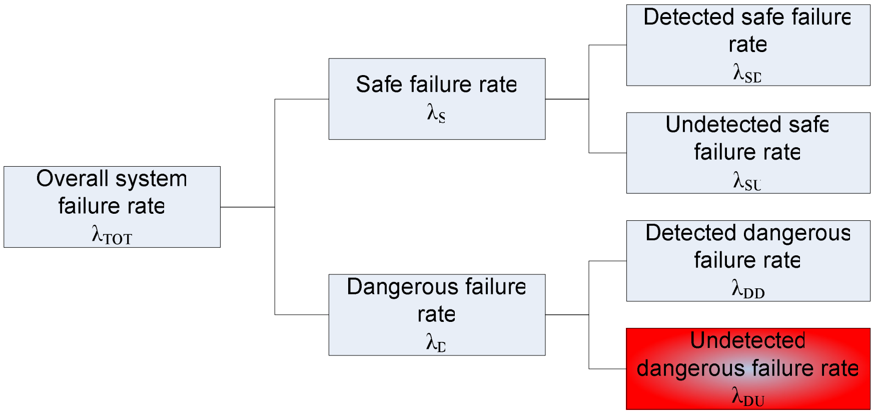

Overall system failure rate λ_{TOT}
Safe failure rate λ_S
Dangerous failure rate λ_D
Detected safe failure rate λ_{SD}
Undetected safe failure rate λ_{SU}
Detected dangerous failure rate λ_{DD}
Undetected dangerous failure rate λ_{DU}

Figure 11 Safe failure fraction classification

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_{TOT}} = 1 - \frac{\sum \lambda_{DU}}{\sum \lambda_{TOT}} \qquad \textbf{(5)}$$

Where:

SFF is safe failure fraction

IEC 61508 dangerous failure rate requirements are introduced in Table 8. [8] Standard requires SFF to be over certain limits in corresponding integrity level. With complex control systems type B requirements should be used, since there is always some uncertainty in behavior under fault conditions.

Table 8 Safe failure fraction requirements for type B systems [8]

Safe failure fraction	**Hardware fault tolerance**		
	0	1	2
<60% (low)	Not allowed	SIL1	SIL2
60-90% (medium)	SIL1	SIL2	SIL3
90-99% (high)	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

Normal machinery control systems do not implement full redundancy. At least some parts of logic system and power supplies are common. Due to that, hardware fault tolerance is 0 in most cases. In practice safe failure fraction should be over 90% in most systems.

4.2.3. Common cause failure

According to IEC61508 hardware related common cause failures arise mainly from two causes. Random hardware failures and systematic failures are two main causes for common cause failures. [8] Both causes are addressed by other requirements also, but common cause analysis address cross linked effects between different channels in redundant or partly redundant systems. Random failures occur randomly over time. Therefore possibility of two simultaneous failures in redundant channels exists, but probability of simultaneous failures is magnitudes lower than probability of one failure. [2]

More important factors for simultaneous failures are related design parameters. For example if cooling is inefficient, both redundant channels might fail due to over heating. It is still quite unlikely to happen at the same time in both channels. In electronic systems diagnostic coverage can be quite high and failure can be detected before second failure. Cycle time of diagnostic functions is important and must be adequate for system and common cause failure mechanisms. [2]

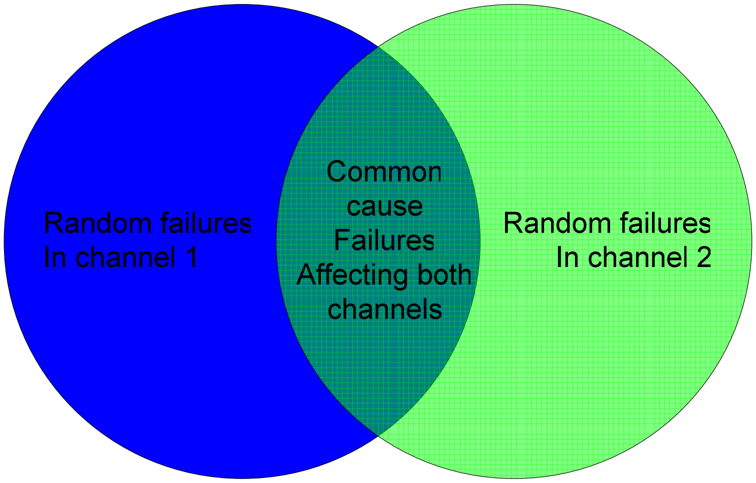


Figure 12 Common cause failure concept

According to IEC61508 there is three major ways to be taken to reduce the probability of dangerous common cause failures:

- Reduce the number of random hardware and systematic failures overall.
- Channel independence should be maximized.
- Fast discovery of single failures [8]

Smith implicates that systematic approach in analyzing of reliability data starts with block diagram level of system and continues with fault three analysis. Good tool for reducing especially dangerous random failures is FMEDA and fault tree analysis. [2] Common mode failures can be quantified with statistical data or by analyzing design features with quantified checklists. ISO 25119 provides a simplified method to analyze common cause failures. Used method is score card in table format. Score card should be used as checkbox. Either result is full score or zero. Approximately one third of the score is related to system concept design. Second third addresses training and competence of personnel of the design company. Last 35% is dedicated to environmental testing rigor. Score from Table 9 should be over 65%. Otherwise additional measures should be applied. More detailed tables can be found on IEC 61508 [8].

Table 9 Common cause estimation score card

No.	**Measure against CCF**	**Score MAX %**
1	**Separation / segmentation**	
	Physical separation between signal and power paths?	15
2	**Diversity**	
	Different technologies/design or physical principles applied?	20
3	**Design / application / experience**	
3.1	Protection against over-voltage, over-pressure, over-current	15
3.2	Selected components are successful proven for several years under consideration of environmental conditions?	5
4	**Assessment / analysis**	
	Are the results of a failure mode and effect analysis (FMEA) taken into account to avoid common cause failures in design?	5
5	**Competence / training**	
	Are designers/ technicians trained to understand the causes and consequences of common cause failures?	5
6	**Environmental**	
6.1	EMC	
	Has the system been checked for EMC-aspects (e.g. as specified in relevant product standards)?	25
6.2	Other influences	
	Are the requirements for immunity to all relevant environmental influences like, temperature, shock, vibration, humidity (e.g. as specified in relevant standards e.g. ISO 15003) considered?	10

4.3. Architectural constrains

Standards describe typical architectures for safety systems. For example ISO 25119 specifies 5 architectures for safety critical vehicle systems. Architectures differ from monitoring and redundancy point of view. Architectures are called as hardware categories. In addition standard emphasizes the need for certain measures for all architectures. Design should implement adequate separation to avoid short circuits. Over dimensioning of components should take place when reasonable. Failure mode control should be made with special care. Cross effects between blocks should be analyzed and isolated. Using of well tried solutions on component and block level is highly recommended. [9]

Categories B and 1 (Figure 13) can be used typically in places where severe injury can happen seldom and operator will most probably avoid hazard anyway. In the other words failure in safety function should not lead directly to catastrophic consequences. [9] In categories B and 1 single failure can lead to loss of safety function and they are not suitable for single point fail operation systems. Category 1 has higher MTTF than B. Diagnostic coverage in both categories is reasonably low, 1 has higher coverage than B.

Properties:

- Inputs and outputs have little or no fault detection.
- Diagnostic coverage is from low to medium
- MTTF for channel varies from low (B) to medium (1)
- Redundant channels or inputs might be required to achieve safe state.
- Consideration of common cause failure is not relevant

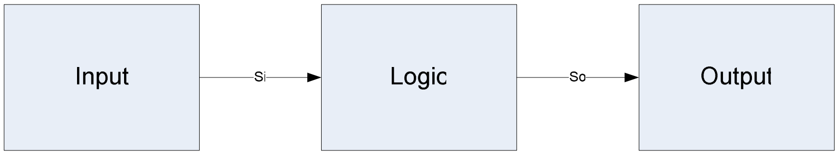


Figure 13 Category B and 1 system

Category 2 (Figure 14) can be used in places where loss of function does not directly lead severe hazard. For example in systems where wrong function could lead to hazard, but no function is considered safe state. Special attention shall be paid to cycle times of diagnostic testing to ensure proper reaction during failure state. Automated testing is preferred, but also manual test routines are allowed. System should maintain safe state until failure is cleared. [9] In category 2 implementation safety function might be lost due to single fail, but safe state is achieved. Test equipment can be external or internal to the unit. Adequate measures to avoid failures conveying from one side to another shall be implemented. Category 2 implementation cannot be used single point failure systems.

Properties:

- Input and output failures are detected in logic elements.
- Diagnostic coverage for device is medium.
- MTTF for channel is from low to medium
- Redundant channels or inputs might be required to achieve safe state.
- Consideration of common cause failure is not relevant
- Output configuration to be arranged in adequate way to avoid hazard in all situations.
- In most cases operator needs to be warned about failure.

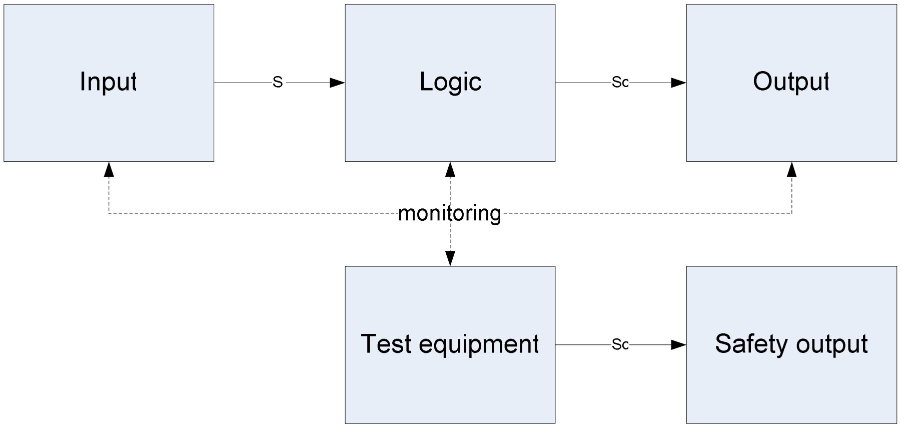


Figure 14 Category 2 system

Category 3 (Figure 15) device can perform safety function even during single failure situation. Category 3 devices can be used single point failure operational systems when adequate power supply schemes are implemented. Proper channel isolation should be implemented to avoid domino effects.

Properties:

- Input and output failures are detected in logic elements.
- Diagnostic coverage for device is medium.
- MTTF for channel is from low to medium.
- Redundant inputs might be required to achieve safe state.
- Redundant outputs might be required to achieve safe state.
- Common cause failures should be taken into account
- Output configuration to be arranged in adequate way to avoid hazard in all situations.
- In most cases operator need to be warned about failure.

Special measures should be made to avoid hazardous failure after single failure situation. Operator should get warning and service request made. Also risk for additional failures shall be included to design calculations and reduced functionality operation limits set. Diagnostic test cycle and periodic proof testing shall be defined. [9]

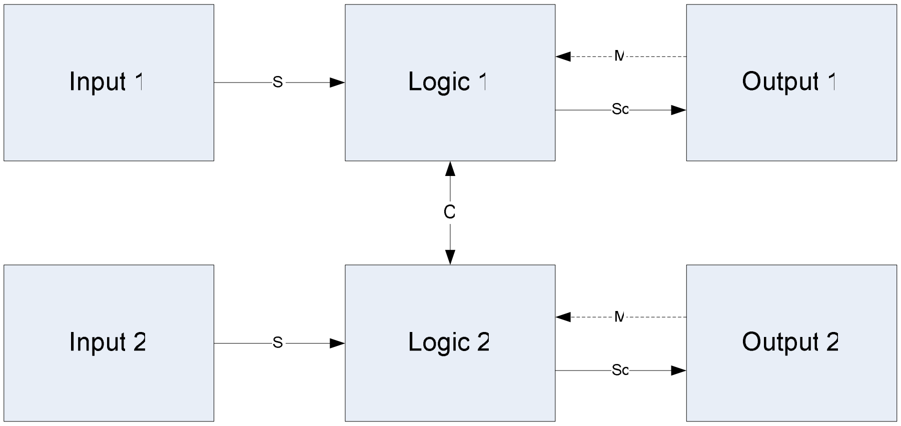


Figure 15 Category 3 system

Category 4 is similar to Cat3 from functional point of view, but needs more rigor in design work and higher reliability. Output monitoring coverage should be higher and MTTF shall be higher than in category 3.

4.4. System behavior on fault detection

System behavior under failure condition shall ensure safe state for system until failure condition is removed. First major consideration is, if system or subsystem is failure tolerant or non failure tolerant. In failure tolerant systems continued operation is allowed during predetermined repair time. Unless repaired in allowed time, switch to safe state is required. Non-fault tolerant systems shall be driven to safe state or low demand rate operation is allowed during repair time. Low demand rate operation calls for additional safety measures. For example manual operation can be allowed during repair time. [2]

In general most mobile ground systems do not have fixed repair times and therefore repair time shall be assumed as infinite. Sometimes reduced operation is needed and it might even be safer than no operation in some cases. For example a main engine in marine environment shall be operational under almost any condition. System design shall be made in a way to allow needed low demand operational modes like manual operation. In addition repair time in marine environment can be arranged to be quite short with on board spares for electronic systems. In general design considerations should be as simple possible to avoid specification mistakes under failure conditions. Most of the systems should be designed to be safe under reset or off conditions. In electronic systems reset is quite often most reliable and easy way to ensure defined state for electronic subsystems

5. MODELING TOOLS

Fault tree can be used to model failure mode logics and also to estimate system failure rates based on known start events. They are often modeling failure of one system block. Failure rate analysis is intuitive from fault tree. When doing failure rate analysis with fault tree, common cause failure modes should be taken into account. Common cause should be taken into account only in redundant channels. [13] Fault tree is a system level modeling tool and proposed failure rate goals can be tested for system. Verification of block level failure rates should be done on component level and failures analyzed in detail with failure mode and effect analysis. Also diagnostic coverage and criticality should be analyzed. (FMEDA) [13]

5.1. Fault tree analysis

Fault tree is a graphical method to describe combinations of events leading to an end event in the top of the tree. Fault tree method is based on using two main logical configurations OR and AND gate. In addition also voted gates can be used. [13] Gates in Figure 16 work as basic logic gates. They can have as many inputs as need and as many series levels as necessary to achieve top event. Basic AND gate latches event trough only when all inputs are active. OR gate latches event trough when any input is active. Start events and result boxes are end points of the chain.[13]

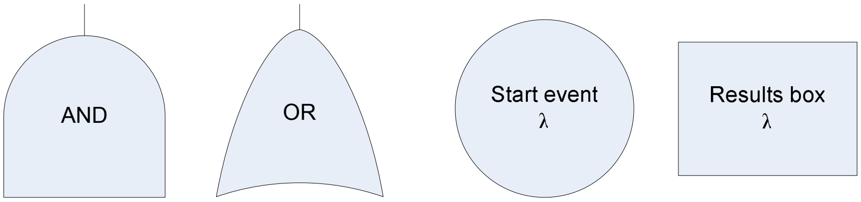


Figure 16 fault tree basic gates

Both voting gates in Figure 17 end up producing same results. Both forms are used in literature. Smith uses voting AND and voting or is used in other reference. In both cases output is true, if required amount of inputs are true. For example in Figure 17 output is true, if two inputs out of three are true. [13]

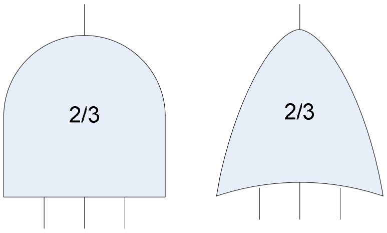


Figure 17 fault tree voting gates

Equation to calculate failure rate after AND gate:

$$\lambda_{and} = \lambda_1 * \lambda_2 \tag{6}$$

Equation to calculate failure rate after OR gate:

$$\lambda_{tot} = \lambda_{and} + \lambda_{cc} \tag{7}$$

Figure 18 describes basic example of fault tree structure and illustrates the effect of common cause failure. Common cause failure has major impact to overall failure rate, since OR causes summation of failure rates instead of multiplying them. Basic statistical calculations can be applied.

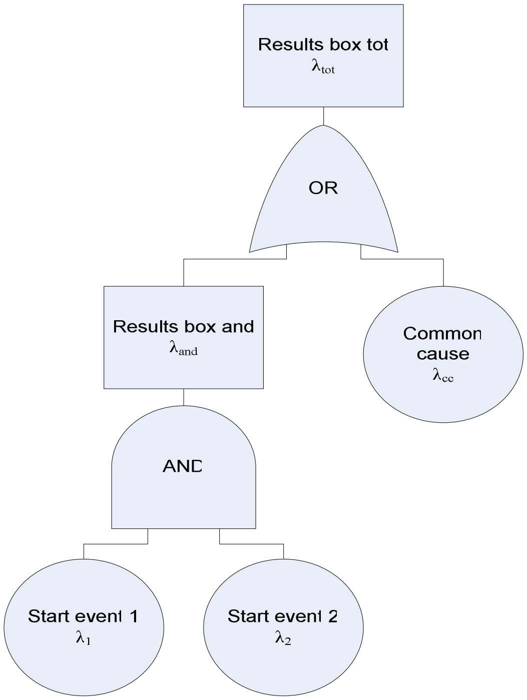


Figure 18 Example of fault tree failure rate analysis

5.2. Failure mode and effect analysis

Analysis can be made on different levels. Failure mode and effect analysis (FMEA) can be made on block level during concept phase to estimate reliability potential of concept. Detailed failure mode and effects analysis with added criticality and diagnostics estimates (FMEDA) made on component level address two areas of safety requirements. Dangerous failure rate requirements can be demonstrated. Secondly thorough criticality estimate addresses diagnostic coverage and safe failure fraction requirements. Distribution failure modes can be obtained from manufacturers and some failure rate sources provide it. Table 10 provides example of FMEDA calculation.

Table 10 Example of failure mode analysis with criticality and diagnostics estimates

Part	Failure mode	Effect	Criticality	Detectability	Overall failure rate	Distribution
Res1	Short	Zero value	Dangerous	Detectable	100	0,1
	Open	High value	Safe	Detectable		0,8
	Drift	Wrong value	Dangerous	Undetectable		0,1

During concept phase analysis can be started on block level. After detailed design component level analysis work as design tool. They also provide evidence of safety integrity level for dangerous failures and safe failure fraction. Failure mode analysis should be used as living and evolving document during development project. [2]

Failure rate estimates random hardware failures. Overall failure rate model is composed from random failures, early failures and wear out. Failure rate analysis quantifies sufficiently constant failures rates in mid life of product. The effect of early failures should be addressed with burn-in testing or extra precautions during commissioning. Product life cycle in safety critical applications shall be limited, since wear out failures should be prevented. [2] Early failure rate period can be also estimated. For example SN 29500 predicts following failure rates for integrated circuits in early failure period introduced in Table 11. [12]

Table 11 Effect of early failures to overall failure rates

Operating time in hours	Increased failure rate factor
0-100	2,9
100-1000	2,2
1000-3000	1,3
3000-	1

From the Table 11 can be seen, that early failures have significant effect during first 1000 hours of equipment usage. Wear out failure prediction should be made based on component data from suppliers. Component reliability data addresses constant failure rate region of bathtub curve. (Figure 19) In practice constant failure rate region is composed from all three failure types, but it is dominated by random failures. It is assumed that safety critical equipments are used during constant failure rate region. [2]

Failure rate data is based on analysis from usage history of components. There are several sources for data and difference in rates between sources is significant. Most common source in the past has been MIL-HDBK-217F. It is released by US Department of Defense. Notice 2 has been released 1995 and especially integrated circuits have evolved much after its release. [2] Several other organizations have updated failure rate collections. In this study electronic component failure rates are referred to Siemens standard SN 29500. It is recommended by several organizations in Europe like TÜV Nord in Germany. General idea in both above mentioned failure rate sources is to provide basic failure rate for component type in question. Basic rate is provided in certain operating environment. Conversion to real operating environment is made with correlation factors.

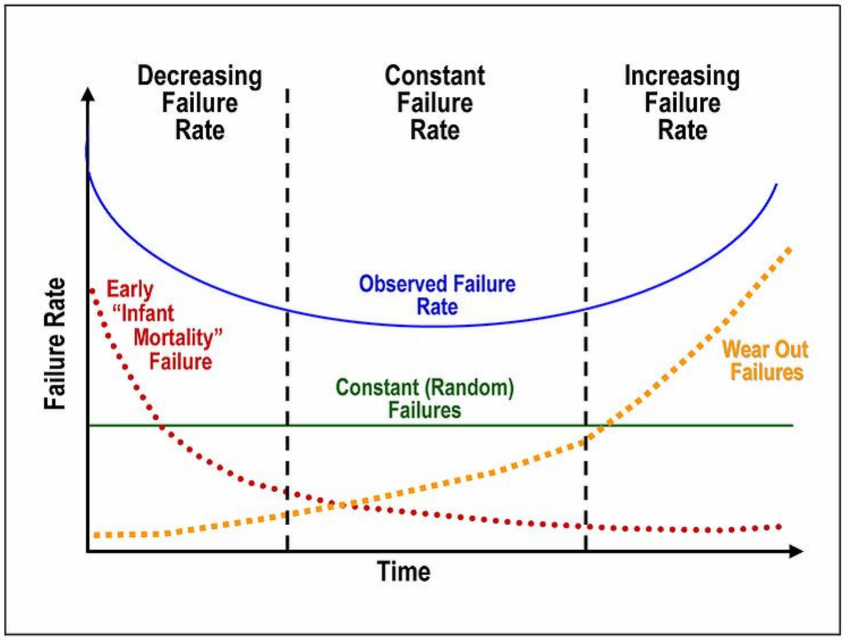


Figure 19 Failure rate bathtub curve

SN 29500 failure rate can be calculated with equation 8:

$$\lambda = \lambda_{ref} * \pi_U * \pi_I * \pi_T \qquad \textbf{(8)}$$

Where:

λ is actual failure rate

λ_{ref} is failure rate basic level (reference)

π_U is voltage dependence factor

π_I is current dependence factor

π_T is temperature dependence factor

Common cause failure rate analysis shall be taken into account in failure tolerant redundant systems. Modeling of common cause failure rate takes individual channel failure rates into account as redundant channels, but common cause failure rate is in series with combined failure rate of two redundant channels (Figure 20).

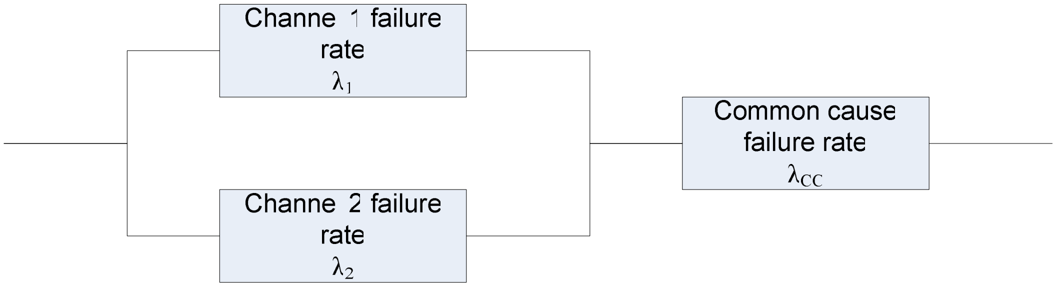


Figure 20 Common cause failure rate model [2]

Equation for combined redundant channels:

$$\lambda_{RC} = \lambda_1 * \lambda_2 \qquad \textbf{(9)}$$

Equation for common cause failure:

$$\lambda_{CC} = \beta(\lambda_1 + \lambda_2) \qquad \textbf{(10)}$$

Where:

β is common cause factor

Equation for total failure rate:

$$\begin{aligned} \lambda_{tot} &= \lambda_{RC} + \lambda_{CC} \rightarrow \\ \lambda_{tot} &= \lambda_1 * \lambda_2 + \beta(\lambda_1 + \lambda_2) \end{aligned} \qquad \textbf{(11)}$$

Failure rate model for redundant channels is calculated as AND-gate in fault tree model with equation 6. Failure rate model for combined common cause and individual failure is calculated as OR-gate in fault tree model with equation 7. Common cause failure rate is substituted with equation 10.

β varies typically between 0,1 to 0,005 depending from environment, system and application. Exact analyzing of common cause failures is not possible. Estimates can be obtained from statistical calculation software's or IEC 61508 part6 Annex D calculation tables. In redundant systems common cause failure starts to dominate failure rate estimates like for example in symmetrical redundant two channel systems. [2]

According to Smith after describing exact looking methods to model failure rates word of warning is needed:

"Because failure rate is, probably, the least precise engineering parameter, it is important to bear in mind the limitations of reliability prediction." [2]

Equations and precise failure rate presented in failure rata data collections implies to precision, but in reality they only give guidance and comparison values for designs.

6. MACHINERY CONTROL SYSTEM

Analysis is made from vehicle graphical user interface and from typical automation sensor interfaces. Main focus on study is to develop concept for controlling safety critical features with graphical user interface. Detailed implementation and design of system is excluded from study to limit needed time and scope. Case study shall be used as a coaching and test case for development process and documentation. Notes and lessons learned shall be implemented to improve development cycle for the development of actual safety system.

6.1. System requirements

Graphical user interface is controlling safety critical vehicle functions trough communication to Electronic Control Units (ECU) actuating hydraulics or other types of actuators. ECU's are designed to fulfill safety requirements and additional needed safety layers shall be achieved trough system concept. The terminal allows a user to safely make conscious commands. Rest of the system would perform the required function safely. However operator should in some case to able to override some safety limits. For example when using tractor as a wheel loader, operator must be able to lower bucket to ground. In some other situations it can be hazardous. To fulfill system level safety requirements user interface must be safe enough.

System concept is constructed from at least two electronic units. One unit is acting as a human machine interface device (later referred as HMI device) and one or more units as a machinery electronics control units (later referred as ECU unit). System has two Controller Area Network (CAN) interfaces. One port is for non-safety critical communication and safety CAN is dedicated to safety critical communication. System side is simplified in picture. In reality CAN networks are distributed to more than one ECU.

The system safety concept as illustrated in Figure 21 will be able to supervise safety critical functions as well as allow use of non-safety critical functions. HMI shall verify correctness of safety command. Correctness of safety command has two major requirements. Command was done consciously and particular command was intended to be executed. ECU shall verify that command is allowed under present conditions. For example implement detaching is never allowed when vehicle is moving. Conditions can wary over operational states. For example during road passage tractor front loader is inactive, but sometimes some functions are allowed under increased caution like using front loader in snow cleaning. In practical systems internal errors cause significant source of failures. Internal monitoring shall be implemented in both HMI and ECU. Additional layer of safety can be achieved by crosschecking between HMI and ECU. Functional requirements are specified in Parker Vansco Display Platform Advanced (DPA) high level specification. [22]

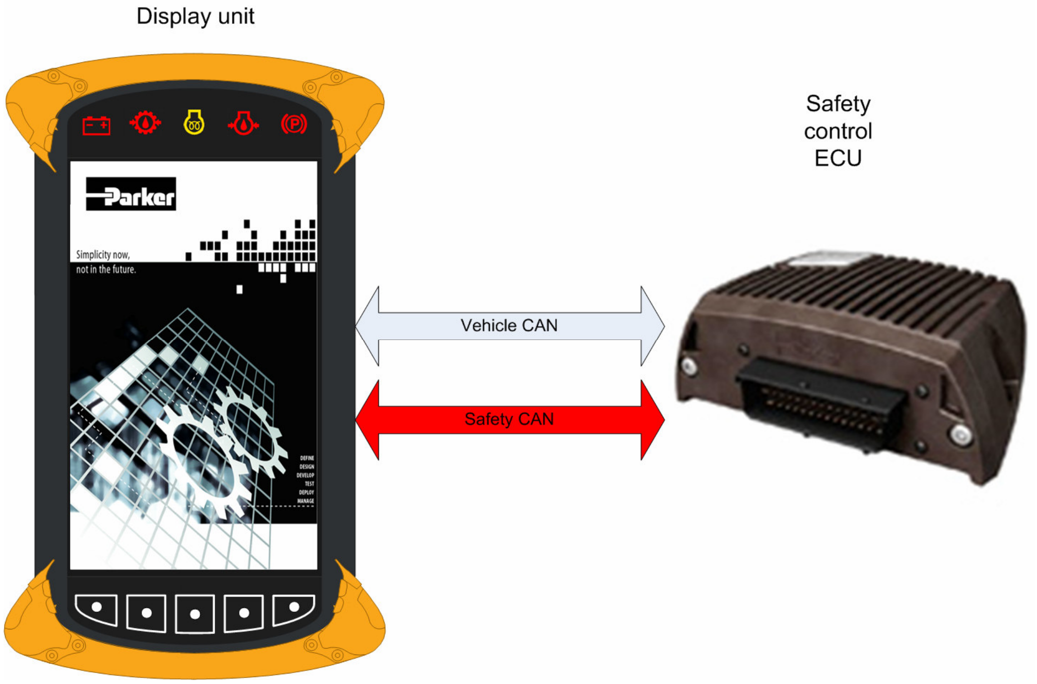


Figure 21 Machinery control system high level concept

Control of safety critical functions

"The operator will be able to enable or disable safety critical functions from the menu system. The user interface will be check-box type graphical object with one fixed color and font size. The location of checkbox graphical object in menu system will be fixed (safety critical graphical object cannot be located inside dynamic scrollable list)".[22]

Figure 22 is simplified state description of command and execute sequence. White states are start and idle stages. Blue states require input from operator and green states operator sees as the end result. Erroneous action by the operator leads to red stages. HMI error is caused by illogical command action and ECU error by violation system stage conditions.

For simplicity internal monitoring and error stages are ignored from system level concept. Sometimes also two way communication is needed to insure safety. For example activation of front loader in vehicle while moving should be verified from operator. ECU shall send request for exception of normal safety operation and HMI notifies operator. Operator input shall be verified and processed as in Figure 22.

Difference between non-safety command and safety command is significant. Non-safety command can be implement with 9 stages and safety command needs 17 stages. System implementation needs also additional stages for internal monitoring.

Safety requires increased complexity of design. Complexity of design increases possibilities for systematic and random failures.

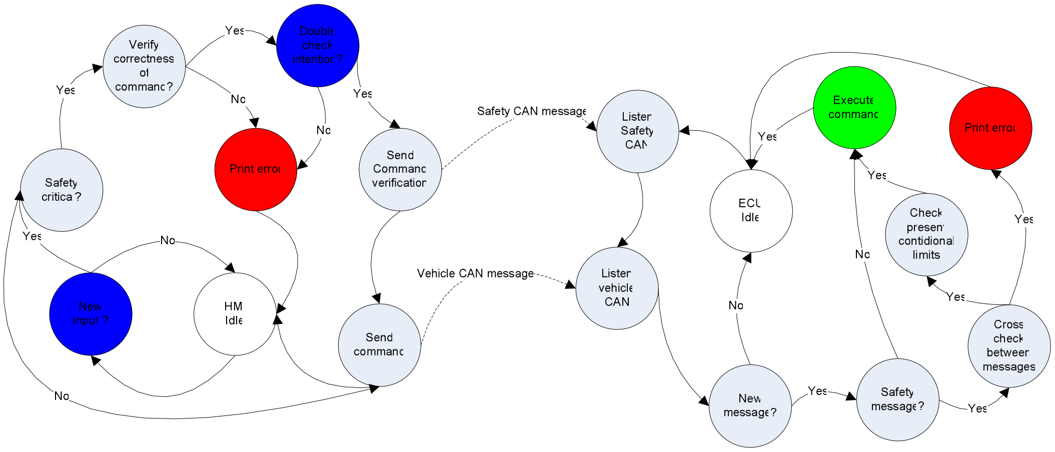


Figure 22 Concept for implementing safety critical operator command

Control of safety critical parameters

"The operator will be able to adjust safety critical parameters from menu system. The parameter adjustment will have limits (min, max) or group of values. The user interface will be an up/down editor graphical object with one fixed color and font size. The location of up/down editor graphical object in menu system will be fixed." [22]

Parameter management follows also Figure 22 procedure in high level, but execution of command does not lead directly to action in machinery. Only parameters in system are updated. Also realization of command verification shall be different, due to natural difference between adjustment and direct activation.

Safety critical graphical information for operator

"The operator will be able to view safety critical information graphically from the display. The warning indicator symbols will be predefined with fixed size and location in the menu system." [22]

In Figure 23 ECU act as initiator and request HMI to draw information message. HMI shall verify that operator will react to message. ECU shall initiate message request when any condition in system needs operator attendance. Typically this is used when condition does not lead to direct safety hazard, but risk is elevated for some reason. For example activation of front loader control while vehicle is moving leads to this kind of condition. Operator verifies that front loader operation is really intentional.

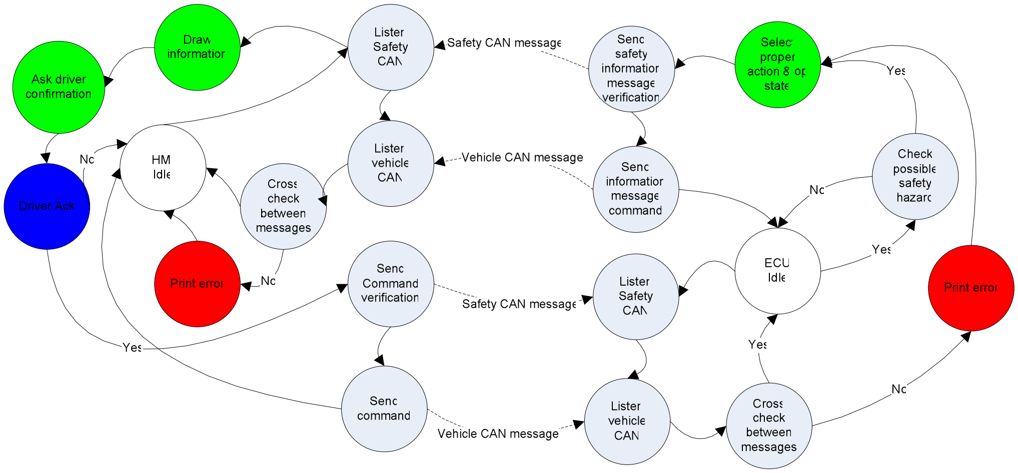


Figure 23 Concept for implementing safety critical information message

Safety critical warnings for operator

As a visual warning the operator will be able to view safety critical telltale LED's above the LCD display. The graphics of the overlay and the color of the telltale LED are predefined. One telltale is dedicated for safety critical warnings. Safety critical sound warnings for the operator shall be implemented with warning tones from buzzer. Combined visual and sound warnings have build in redundancy. [22]

Activation of operator warnings follows Figure 23 concept, but uses dedicated safety warning methods in combination to draw operator attention. It is used when system conditions lead to direct safety hazard. It could be for example internal error in safety related mechanical or electrical systems.

System level safety analyzing is done briefly and straight forward, since it is not the main focus in this study. It is intended to provide background information and starting point for low level analysis. System level analysis should be done or approved by OEM. First step was to figure out safety critical functions in equipment under control.

Safety critical functions related to HMI:

- View machine information graphically from the display
- View machine information visually from telltales
- Safely enable / disable machine functions
- Play warning sounds

In real application the amount of functions shall be higher and especially they should be described in more detail. Risk analysis was made to figure out failure modes and their severity, likelihood of exposure and possibilities to control damages. Results in Table 12 were formed based on chapter 3.1. From Table 12 needed safety integrity levels were concluded with risk graph approach. Risk graph used was based on Figure 6.

All failures might lead to injury of bystander or operator, but quite rarely to death. Control errors are considered more likely than signaling errors, since signaling error does not lead necessarily to hazardous situation. Most of the failures as such are not controllable, but distorted or black display is considered to be more likely to be noticed.

AgPL levels based on Table 13 are b and c. Levels b and c do not require any particularly strict safety features. They can be achieved with quite basic changes to present control systems. Category 2 was selected, because qualitative requirements for display software in self monitoring category 1 were considered to be unachievable.

Display operating system was selected to be Linux based and safety assessment of open source software is in reality impossible. Use of open source code directly in safety critical system without individual monitoring requires full coverage testing and full coverage in testing is hard to achieve. However reliability as such is quite good in Linux based systems due to wide usage. Category 2 is illustrated in Figure 14. Table 14 shows that required SIL is 2 at maximum. Qualitative requirements can be achieved with reasonable improvements to present development process. Main effort should be paid to structured specification and documentation of every step in process. SIL 2 levels are achievable with traditional tools and improved methods. Safety plans and some checklists are needed as additional features to process. Also design guides must be reviewed. High level changes are included to assessment checklist in Appendix A.

Table 12 Risk analyzes for HMI related functions

Function	Failure	Severity	Exposure	Controllability
Safety critical vehicle function control	Graphical display error	S2	E3	C3
	Menu control error	S2	E3	C3
	Parameter adjust error	S2	E3	C3
	Communication timing error	S2	E2	C3
	Communication content error	S2	E2	C3
Display warning symbols graphically	Graphical display error	S2	E3	C2
Display signals with telltales	No telltale	S2	E2	C3
	Wrong telltale	S2	E2	C3
Play warning sounds	No sound	S2	E2	C3

Table 13 Safety integrity targets based on risk graph

Function	Failure	Ag PL
Safety critical vehicle function control	Graphical display error	c
	Menu control error	c
	Communication timing error	b
	Communication content error	b
Display warning symbols graphically	Graphical display error	b
Display signals with telltales	No telltale	b
	Wrong telltale	b
Play warning sounds	No sound	b

Table 14 Overall safety integrity levels for system based on category

Function	Failure	Cat	SRL (SIL)
Safety critical vehicle function control	Graphical display error	2	1
	Menu control error	1	1
	Parameter adjust error	1	2
	Communication timing error	2	2
	Communication content error	2	B
Display warning symbols graphically	Graphical display error	2	B
Display signals with telltales	No telltale	1	1
	Wrong telltale	1	1
Play warning sounds	No sound	1	1

6.2. Human Machine Interface

Graphical operator interfaces have become more attractive due to increased complexity in machinery controls. It is not very ergonomic to have tenths of buttons and levers for example in ships bridge or tractor cabin. In quite many cases required control tasks and series are complex. For example when turning tractor and implement around in the end of the field during cultivating, operator need handle implement functions, control hydraulics, change gears and turn the wheel. Also handling of ship based on real time positioning in oil field tasks is impossible when implemented with several independent levers. Automation of some tasks improves ergonomics greatly. Operator can for example make macro for handling implement and hydraulics and start macro when reaching the end of field. Automation of vehicle control systems leads to need of reliable and safe electrical system. It could be very dangerous to drop down the implement during road passage for example.

HMI device layout in Figure 24 provides graphical user interface with information indication capabilities. Warning telltales with buzzer provide direct method to alarm operator in case of hazardous situation. Rotary encoder and four push buttons on bottom of unit allow efficient and easy menu navigation for operator. Side panel push buttons provide method to verify operator inputs with redundant device. This leads to a safe and user friendly HMI. Based on system requirements the operator needs to be able to perform Table 15 functions from the user interface. In the study focus is on analyzes of two safety functions, since they cover most of the interesting safety issues. ***Safely enable / disable machine functions*** and Hear warning tones are covered in following analyze.

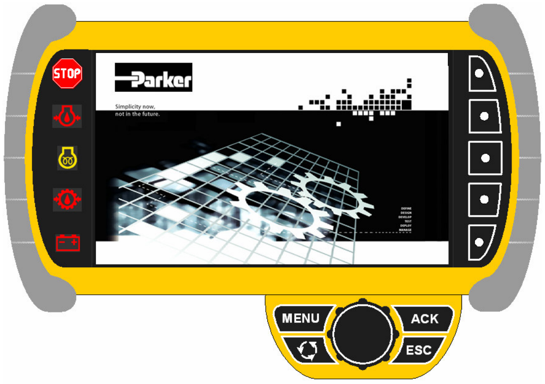


Figure 24 Possible layout for safe machinery control system HMI device

Table 15 HMI functional requirements

Required function	Criticality classification
Adjust display brightness	Safety related
View and adjust the time of day from the display	Non-safety
View machine information graphically from the display	Safety
View machine information visually from telltales	Safety
Safely enable / disable machine functions	Safety
Manage user settings	Safety related
Manage diagnostic log (with timestamps)	Non-safety
Manage machine calibrations	Safety related
Perform service functions (e.g. read service manual, data logging)	Non-safety
Hear warning tones	Safety
Audio / video playback (e.g. mpeg, mp3)	Non-safety

Safely enable / disable machine functions

Safe machine function control has two high level requirements. First is to verify operator intend. Second is to control internal errors. In the other words right function shall be commanded when intended. Operator intend is human error type failure and impossible to fully prohibit, but adequate measures shall be used to decrease likelihood. Internal errors shall be monitored with internal monitoring circuitry. Implementation uses secondary confirmation to address human errors. Operator shall be prompted to assure right intention. Internal monitoring scans menu actions made with main user interface. Display data shall be verified by internal monitoring.

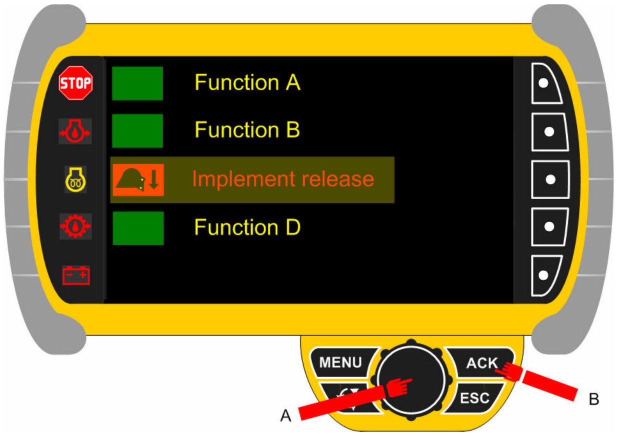


Figure 25 Menu item selection

Figure 25 shows typical menu control event. Rotary (A) encoder shall select function from list. Operator can activate highlighted selection with ACK (B) button. All safety functions shall have for example red text color and picture with red background. Menu selection user interface uses external keyboard device. Device is connected to main controller with serial interface. Also internal monitoring system shall have monitoring port for this serial interface. Monitoring checks correct menu position from main controller and makes display data check.

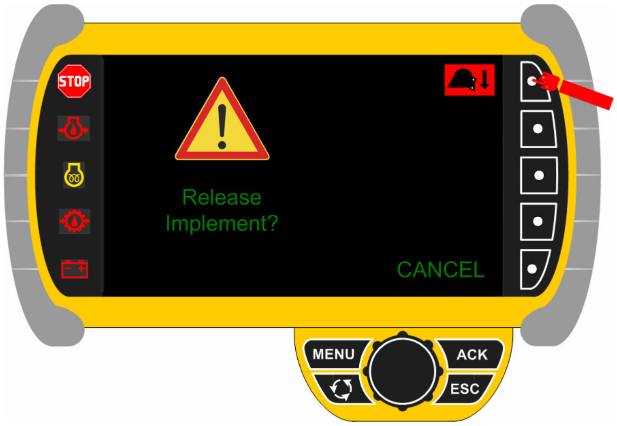


Figure 26 Safety item confirmation

Operator confirmation shall be verified with additional check after critical item selection. Operator must accept activation of functionality twice. Second accept shall be handled with different input device as in Figure 26. Function must be accepted within specified time window or it will be automatically cancelled. Secondary input device is connected to monitoring device and main controller has no control over it. Device is simple push button keypad. Timing of operator action is controlled with signal edges. Both signal transitions must fit to timing windows. Activation of signal should be inside specified timing window. Delay between activation and release must be adequate compared with typical human action.

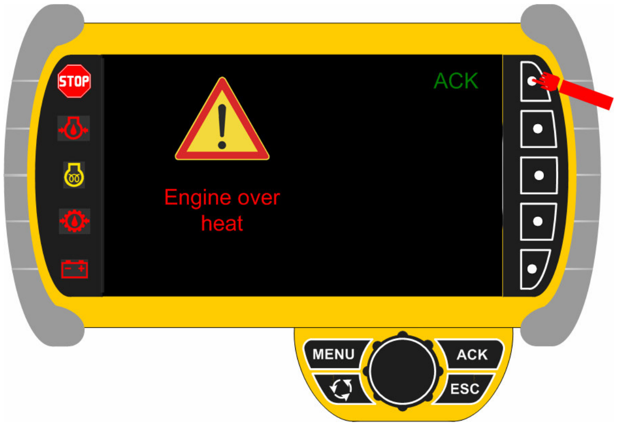


Figure 27 Operator alarm display example

Operator alarm

Operator alarm can be triggered from systems via serial communication or HMI internal error could lead to alarm. Alarm should draw operator's attention and needs to be confirmed with keypad activation as in Figure 27. During operator alarm stage warning symbol on display and stop telltale led flashes to draw operators attention. As an additional safety feature buzzer sound shall be used until alarm is acknowledged by operator. Using stop telltale and display symbol simultaneously with buzzer sound provides safety redundancy.

6.3. Control ECU

Typical ECU has sensor interfaces, actuator control outputs and communication ports. In machinery-control-systems sensors convert physical quantities to electronic signals. ECU converts electric signal back to physical quantity with signal conditioning and AD-conversion. Units are connected to each other with CAN field bus. ECU actuator ports drive often solenoid type loads to control fluid flow or transform electric force to mechanical force. ECU designs are application specific and focus here is to provide only general ideas. Safety critical ECU system designs follow often architectural categories 2 or 3 presented in Figure 14. Control modules form a heart of safety systems and are responsible for safe operation of machinery.

Reliable sensor interface requires diagnostics from whole circuitry. In most cases safe system design calls for redundant sensors. In some cases it is enough to diagnose failure in sensor and use safe default values to operate system. Attention should be paid to make sensors easily diagnosable. For example knock detection is very critical measurement in modern medium speed natural gas engine. Based on physics Otto cycle internal combustion engine fuel economy is best at knocking border. Active knock detection helps on approaching that border. Crossing that border causes risk of mechanical failure to engine and eventually a life threatening situation to people close to engine. Traditional knock detection method is very simple. Piezo-electric vibration sensor is used and AC-coupled signal is filtered and integrated to measure signal level on certain frequency range. [17] In basic circuitry sensor is references to ground. DC-level on signal lead is roughly same as ground. If sensor wire breaks, DC-level stay still on same level. Measurement result during wire break is same as internal noise on dedicated frequency range. This will be interpreted as no knock and wire break is not noticed. Control algorithm drives engine over the knock border, since knocking is not noticed.

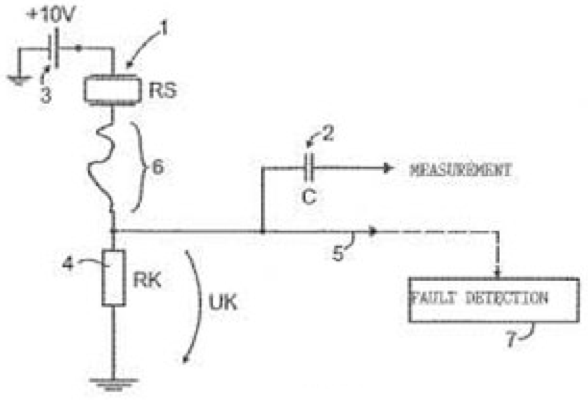
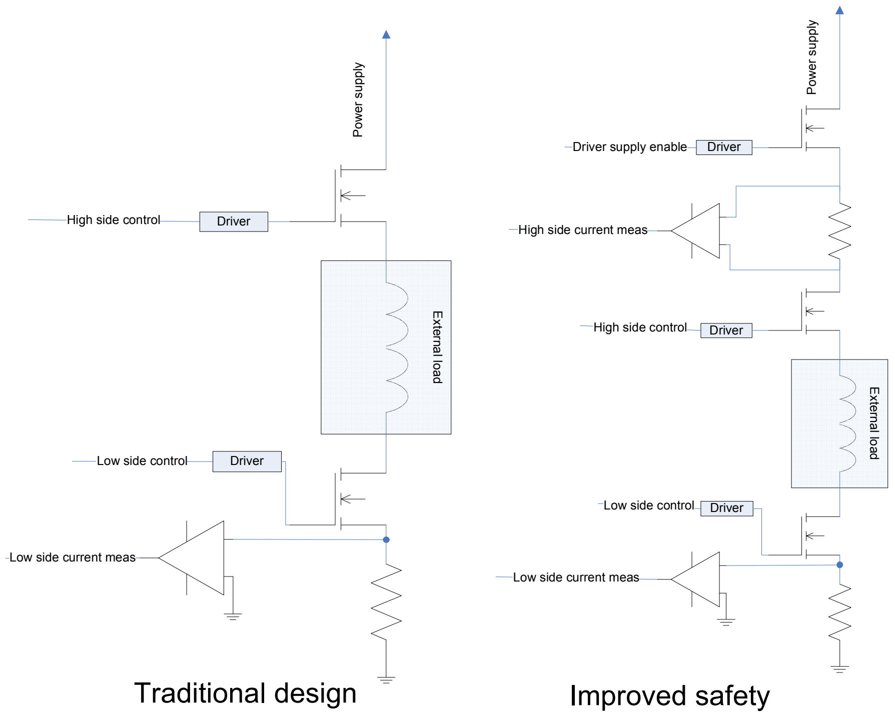


Figure 28 Patented improved knock detection sensor diagnostics [21]

Diagnostics of piezo-electric signal can be quite easily improved with predetermined reference level on sensor reference lead as in Figure 28. Sensors have series resistance of around 1MΩ. With additional pull down resistor signal lead DC-level can be set above ground level. DC-level does not need to be accurate. Wire is considered to be intact until DC-level is close to zero. Fault detection circuitry indicates failure to ECU CPU and operation with safe default values can be continued. This idea has been developed by design team including Parker Vansco and Wärtsilä engineers and patented by Wärtsilä. [21] Two redundant sensors can be used in systems were limiting of values like temperature is needed. If limit is reached by any of the sensors, system shall be forced to safe mode. If actual values are needed to operate system on any mode, sensor voting systems shall be used. In general highly dependable system should incorporate smart sensors and interfaces when possible. For example serial interface sensor with internal diagnostics would make system design easier. [18]

Communication with field bus protocols is quite reliable. For example CAN bus specification include message CRC and reliability mechanisms like acknowledge from receiver to sender. Main concern is physical signal interruptions in bus lines. Redundant bus topologies allow communication rerouting in case of line failure. Also ring topologies could be used for reliable systems to recover from wire breaks.

Actuator drives are most tricky to design to be fail safe. Outputs tend to be also most error prone, since drivers control often significant amounts of energy and there is also power losses related. Actuator drive requirements should be designed to safe OFF type. Otherwise system complexity increases dramatically. For example in battery powered systems dual power grid is needed.



Traditional design

Improved safety

Figure 29 Safety improvements for typical PWM type solenoid drive

Typical solenoid drive needs mainly improvements to diagnostics. It is inherently quite safe due to dual side switches. Diagnostics are improved with dual side current measurement as in Figure 29. Comparison between current levels provides load circuitry integrity diagnostics. With these improvements drive circuitry itself is single fault tolerant. Additional power switch on driver can be used to shut off loads during major failure in unit. In most cases there is only one switch controlling all outputs in unit and it is controlled with independent monitoring circuitry. In category 2 (Figure 14) main control is handled with logic element, but safety monitoring is handled with independent monitoring logic. In most machinery controls category 2 have adequate safety level. Traditional control systems have high diagnostic coverage, because preventative maintenance and dependability is required anyway.

Additional safety measures are needed to reduce risk further. That requires specific monitoring circuitry and review of diagnostic features. Monitoring can be implemented for example with microcontroller. Monitoring must be able force system to safe state with independent ways. Additional power supply switch in Figure 29 provides an independent channel to drive outputs to OFF and safe state. Most demanding challenge for safety system logic design is actually specification and implementation of software, since even in pretty simple control systems chains of events and cross references can became complex. Embedded system software design shall follow strict and appropriate process. In most cases company specific software design process with additional safety related measures works fine. For example Parker Vansco design process described by Salo can be used with some adjustments. [7]

6.4. HMI unit hardware requirements

Display unit includes two types of interfaces. They are divided to human interfaces and system interfaces. Also some miscellaneous interfaces are needed to implement functional requirements. Most of the interfaces are considered as safety critical. Interfaces are illustrated in Figure 30 on black box level. Safety related interfaces to external system have red color. Only Vehicle CAN is considered non safety related. Also vehicle CAN is monitored by safety monitoring, but erroneous operation only on vehicle CAN cannot trigger safety hazard.

Table 16 summarizes HMI unit external interfaces. 7" inches TFT widescreen color display was selected to concept, since market interest seams to move to that direction. Wide spectrum of operating conditions calls for active display. Passive displays have been earlier used in automotive industry, but for example temperature extremes cause more problems to them. Five buttons and telltales fit nicely to mechanical construction on the side of the display. Decision to connect main keyboard to serial interface was done, because quite often better ergonomics are achieved when keyboard is separated. For example in the tractor display could be mounted to dashboard close to window for easy readability while driving and keyboard to armrest where most control buttons and levers are located. Continuous power supply is needed for controlled shut down and key-lock shall wake up or power up the device.

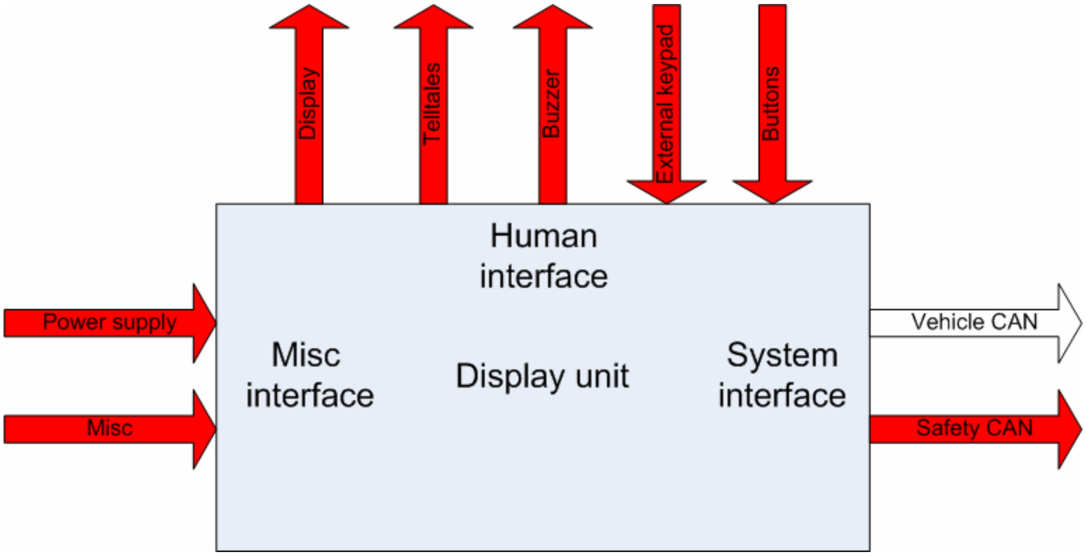


Figure 30 HMI unit hardware requirements

Table 16 HMI unit interface summary

Human interface	
Outputs:	7” WVGA TFT color display
	5 Telltales
	Buzzer
Inputs:	External keyboard with rotary encoder
	5 buttons on display side
System interface	
Communication:	Vehicle CAN
	Safety CAN
Misc:	Power supply
	Keylock

Monitoring requirements are derived from risk analysis in Table 12 and introduced in Table 17. Monitoring of displayed data is done with calculation of CRC over screen area in question. CRC values are calculated during design of vehicle specific menu control structure and stored to monitoring equipment. All safety critical menu items have their own signature CRC. Also human interface devices are monitored and during system specific menu control design correct control commands are parameterized. Parameters are stored to monitoring system. Monitoring of telltale functions is implemented with current diagnostics from illuminated leds. Only those leds which are activated should consume power. Buzzer monitoring is done with buzzer current check.

Table 17 Internal monitoring function examples

Function	Failure	Diagnostics
Safety critical vehicle function control	Graphical display error	Graphic CRC
	Menu control error	Graphic CRC and menu control check
	Parameter adjust error	Graphic CRC and menu control check
	Communication timing error	Communication check
	Communication content error	Communication check
Display warning symbols graphically	Graphical display error	Graphic CRC
Display signals with telltales	No telltale	Internal check with led currents
	Wrong telltale	Internal check with led currents
Play warning sounds	No sound	Internal check with buzzer currents

Structural specification calls for traceability on every level of specification. Starting point for specification is functional requirements. Table 18 shows few examples of traceability chains. Examples are selected to cover functionality to warn the operator. Chains form different kind of structures. Some chains might skip some levels forming shorter chain and in the other hand some requirements could be based on same level requirement. Unambiguousness and traceability combined requires short and clear requirement descriptions especially on lower levels. Requirement descriptions must be measurable to alloy easy testing.

Functional requirement level (FRS) specifies **what** needs to be done and technical requirements level (TRS) tells **how** functions are fulfilled. FRS and TRS specifies unit on black box level and corresponding testing is done from external interfaces. Hardware architecture level (HWA) specifies hardware high level implementation and internal interfaces. Hardware module level (HW with module name) covers detailed module specification.

Basic format used in study for requirement combines four attributes. Requirement is identified by unique name based on structural level and type combined with sequential coding in the end. For example FRS Operational C is highest level (functional) requirement. It is classified as operational, because it is related to module operation with operator. C is unique sequence code for requirement. Requirement source is specified for lower level requirements. Test case provides information how requirement is verified or validated. Description is the actual specification for requirement. It should be simple and include tolerance.

Table 18 Specification structure example

Req.	Source	Test case	Description
FRS level			
FRS Operational C		Safety function validation	Terminal need to be able to warn operator with warning tones / sounds and operator needs to them heavy noisy environment
FRS HMI D		Safety function validation	View machine information graphically from the display (e.g. Gauges, warning indicators) or from common telltales
TRS level			
TRS Diagnostic LED C	FRS HMI D	Integration test	Five telltale Leds for application purpose.
TRS Diagnostic LED D	FRS HMI D	Functional validation	Luminous intensity: over 5000 mcd
TRS Diagnostic LED F	FRS HMI D	System Integration test	As a safety feature fail leds shall have a feedback diagnostics
TRS Buzzer A	FRS Operational C	Functional validation	Sound pressure (1m): over 85 dB
TRS Buzzer B	FRS Operational C	Functional validation	Frequency range: 200-1000 Hz ±10Hz
TRS Buzzer C	FRS Operational C	System Integration test	As a safety feature buzzer shall have a feedback diagnostics
HWA level			
HWA interface LED A	TRS Diagnostic LED C	HW integration test	PWM control for led current
HWA interface LED B	HWA interface LED A	HW integration test	Led PWM resolution better than 1/100
HWA interface LED C	HWA interface LED A	HW integration test	Led PWM frequency higher than 500Hz

HWA interface LED D	TRS Diagnostic LED F	Safety function validation	Analogue led current feedback to monitoring
HWA interface LED E	HWA interface LED D	HW integration test	Analogue led current feedback accuracy ±5%
HWA interface Buzzer A	TRS Buzzer A	Safety function validation	PWM control for buzzer current
HWA interface Buzzer B	HWA interface Buzzer A	HW integration test	Buzzer PWM resolution better than 1/1000
HWA interface Buzzer C	HWA interface Buzzer A	HW integration test	Buzzer PWM frequency higher than 10000Hz
HWA interface Buzzer D	TRS Buzzer A	Safety function validation	Analogue buzzer current feedback to monitoring
HWA interface Buzzer E	HWA interface Buzzer D	HW integration test	Analogue buzzer current feedback accuracy ±5%
HW Module level			
LED A	TRS Diagnostic LED C	Simulation, prototyping or reused circuitry	PWM control for led current
LED B	TRS Diagnostic LED F	Simulation, prototyping or reused circuitry	Current to voltage converter: 0-50mA IN / 0-5V OUT
LED C	TRS Diagnostic LED F	Simulation, prototyping or reused circuitry	Current to voltage converter accuracy ±3%
BUZZER A	TRS Buzzer A	Simulation, prototyping or reused circuitry	PWM control for buzzer current
BUZZER B	TRS Buzzer C	Simulation, prototyping or reused circuitry	Current to voltage converter: 0-200mA IN / 0-5V OUT
BUZZER C	TRS Buzzer C	Simulation, prototyping or reused circuitry	Current to voltage converter accuracy ±3%

Table form of requirements alloys easy traceability with verification matrix formed from requirement tables. Verification matrix can be used in spreadsheet form to filter and follow requirement changes during specification reviewing and changes. Table 18 shows only strict requirement part of specification document. Natural language representation gives designer a better view of requirement and semi formal modeling illustrations as pictures are beneficial. For example Universal Modeling Language (UML) type descriptions are strongly recommended. [14]

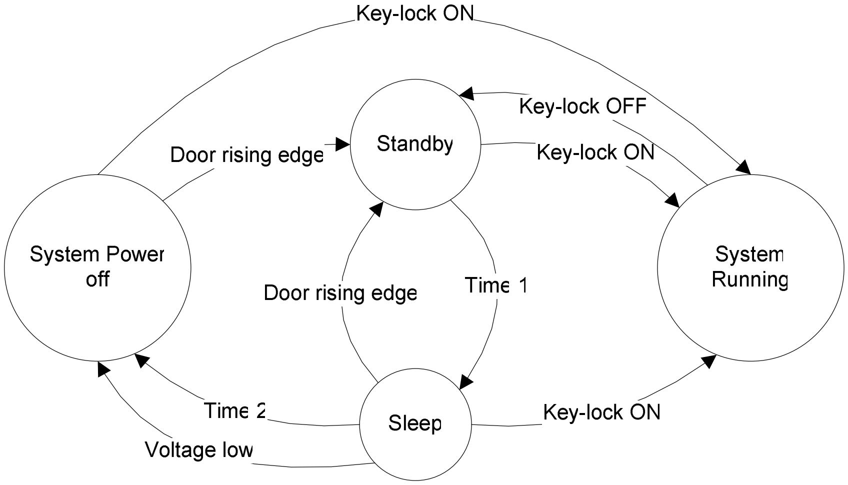


Figure 31 System operational modes

For example operational modes specification in Figure 31 is very illustrative compared to natural language description. It would be really hard to describe unambiguously relations between stages exactly. It is easy to say that system should be ready to run when operator comes to cabin and it should be running when ignition engaged. Sentence above is basic specification, but also returns back from different states need to be specified. Also unexpected situations like operator just visiting cabin and going away has to be considered. Power of modeling languages is in making complex systems more intuitive.

6.5. Implementation concept

Category 2 type implementation uses individual safety monitoring logic as in Figure 32. Test logic can force system to safe state and prevent false triggering of safety critical machine functions. In the other hand operator warnings have redundancy, since warnings can be triggered by main logic or test logic. Communication correctness shall be verified with dual messaging. Messages with safety critical activation commands must be accepted by both logics. Main logic shall use vehicle CAN to transfer messages and test logic must confirm message with safety CAN.

Human interface devices are divided to two blocks. External pointing device and keypad shall be read with main logic and the test logic verifies correctness of main logic menu functions with menu skeleton and pointing device monitoring. Secondary operator confirmations are handled trough side button panel and it is handled trough test logic. Side button actions are communicated to main logic trough test logic.

Visual information to operator shall be handled with dual channels. Main logic controls TFT display and display data is verified by test logic. Display control on main logic side provides CRC from display data blocks when requested and test logic compares values to predetermined values from design tool chain. Telltales can be used as a back up for visual warning to operator. Buzzer provides redundancy for visual warnings and human error.

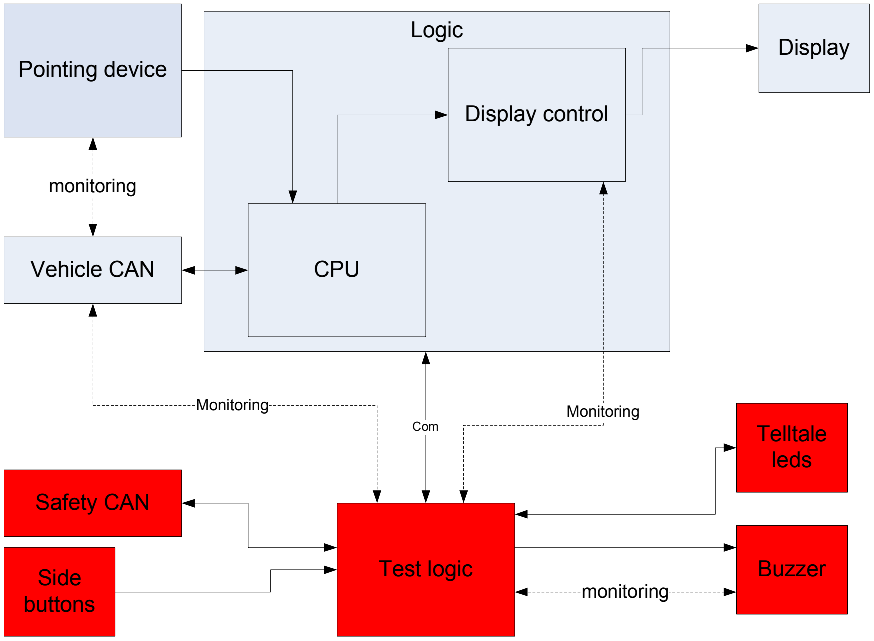


Figure 32 HMI unit hardware concept

Main logic and test logic requires individual power supplies and careful interface design to prevent common cause failures based on common circuitry. All common parts and interfaces shall be well diagnosed to maintain safe state during random failures. Special attention should be paid on power up and down sequences and overall diagnostics of internal functions.

6.6. Failure rate estimates

As described in chapter 4.2 random failures shall be analyzed on circuitry level to get failure rate estimate for single blocks. Then blocks must be combined and total values for channels calculated. Channel estimates shall consider also common cause failures. Random failures for circuitry blocks are calculated with FMEDA method and channel values are based on blocks and estimates of common cause failure risk. Channel values are calculated with fault tree method described in chapter 5.

Estimates were calculated in Table 10 format. Full calculation is in Appendix B. Calculation is example from safety ECU solenoid driver circuitry. Table 19 presents total values for different failure types described in Figure 11. Safe failure fraction for solenoid drive circuitry is 96% based on equation 5. It is reasonably high and adequate for SIL2 design with 0 hardware fault tolerance according to Table 8.

Table 19 FMEDA results

TOTALS	FIT SD	FIT SU	FIT DD	FIT DU
	3200	3170	690	270

Failure rates for individual blocks are not interesting. They must be combined to form whole functional safety channels and common cause failures rate should be estimated. Common cause failure rate estimate is based on Table 9. Table score was calculated to be 75%. Reasoning for score can be read from Table 20. Common cause failure factor β was estimated to be reasonably low, since 75% was quite good result. 0,01 was used for β value in common cause failure rate calculations.

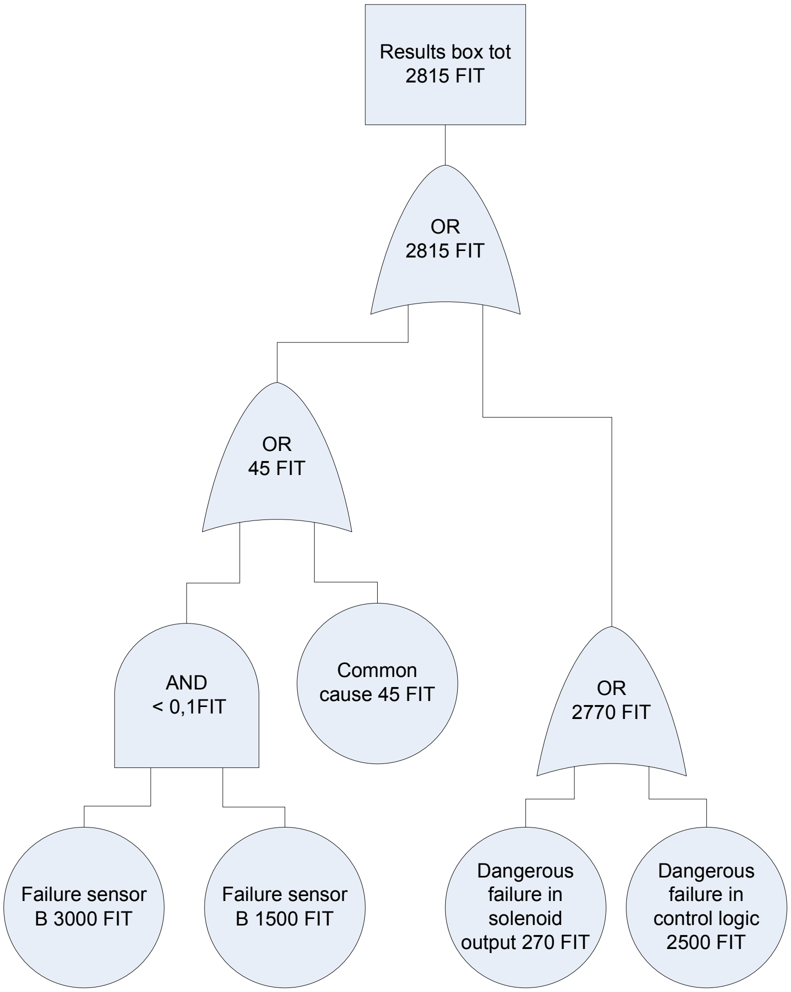


Figure 33 Safety ECU simple control channel failure rate based on fault tree

Figure 33 illustrates combined failure rate for simple control channel example. System controls proportional solenoid valve based on analogue information from two redundant sensors. Sensors use different method to convert physical signal to voltage. System safe state can be achieved with solenoid valve shut off. Due to that single solenoid drive can be used with additional shut down described in chapter 6.3. Failure rates for elements are based on calculation in Appendix B and estimates from SN29500 [12]. From sensor interface example can be seen that common cause dominates redundant channel design failure rate estimates. Control logic causes most of dangerous failures, since it is most complex block in the system. Total failure rate in Figure 33 is 2815 FIT's. For SIL2 level applications FIT under 1000 is required.

Table 20 Common cause estimate for safety ECU

No.	**Measure against CCF**	**Reasoning**	**Score % (YES full score, NO 0)**
1	**Separation / segmentation**		
	Physical separation between signal and power paths?	Same connector for signal and power	0
2	**Diversity**		
	Different technologies/design or physical principles applied?	Different sensor types used in sensor redundancy	20
3	**Design / application / experience**		
3.1	Protection against over-voltage, over-pressure, over-current	Industrial and automotive requirements fulfilled	15
3.2	Selected components are successful proven for several years under consideration of environmental conditions?	New combonets partly used	0
4	**Assessment / analysis**		
	Are the results of a failure mode and effect analysis (FMEA) taken into account to avoid common cause failures in design?	YES	5
5	**Competence / training**		
	Are designers/ technicians trained to understand the causes and consequences of common cause failures?	NO (First safety project)	0
6	**Environmental**		
6.1	EMC		
	Has the system been checked for EMC-aspects (e.g. as specified in relevant product standards)?	Industrial and automotive requirements fulfilled	25
6.2	Other influences		
	Are the requirements for immunity to all relevant environmental influences like, temperature, shock, vibration, humidity (e.g. as specified in relevant standards e.g. ISO 15003) considered?	Industrial and automotive requirements fulfilled	10
		Total	**75**

6.7. Safety assessment

Safety assessment contains review of project deliverables and proposed actions based on reviews. Checklists are powerful tools for assessment work, but main requirement is proper assessor competency. Assessment shall be done by someone who has adequate independence from project organization. Checklist in Appendix A can be used as starting point for company producing machinery-control products. Checklist is adapted from example by Smith. [1]

Checklist describes minimum requirements for SIL2 level systems. Main focus in assessment shall be in qualitative requirements, since level of rigor is not as obvious as with quantitative requirements. Checklist should be used alongside with evidence of fulfilled requirements. In the other words OK can be checked only with proper evidence. In some projects some requirements might be not applicable, but in that case NA should be used. NA needs always explanation for the exception.

Safety assessment cannot be passed in this stage since project is in concept phase. Assessment checklist helps in steering the project to right direction and most tools are used on concept phase to evaluate different approaches. Checklist can be used also as gap analyze for company design process. For example testing is often done, but evidence of testing is not recorded according to safety standard requirements.

In Parker Vansco case structuring of design and documentation is big challenge. Also some design guides should be revised to fulfill all requirements. Validation planning needs attention, since it is often co-operation with customers and responsibilities should be clear. Most requirements are at least partly covered, since Parker Vansco have a company level ISO9001 certificate for operations.

7. RESULTS AND DISCUSSIONS

Dependability can be seen as result from availability, reliability and safety as indicated earlier, but sometimes all three do not walk hand in hand. Analysis techniques address all aspect in general, but required actions after analysis need to have focus to wanted direction. In most cases increased reliability offers also higher availability. Safety requirements sometimes counteract against availability, since in fault conditions availability is reduced because of safety hazards. Safety and reliability requirements easily lead to more complex systems and it might lead to higher need of service. Service time means lowered availability in most cases.

It is important to consider this during concept phase. Safety level targeting needs to be adequate, but not over engineered. Reliability considerations should be made on overall level and without unnecessary complexity. Safety is also application and situation specific issue. It could be hard for design engineer to foresee all possible cross references between different operational situations. For example running ship engine without oil pressure is hazardous situation and might lead to high costs and possible injuries to operator. When ship is sailing on hazardous waters near land, most captains are willing to accept risking engine instead of whole ship anyway. System analyzes should be made with cross functional teams and contracting of design work must made with special care.

Figure 34 illustrates that during concept phase decision of focus point should be set between three attributes of dependability. Safety level is often set by external authorities and customer focus is somewhere between availability and reliability. In reality costs often drive design heavily and especially in sub contracting they are decisive factor. Instead of hardware cost and direct development cost attention should be paid to total costs including whole product life cycle. Most of methods are very efficient also in non-safe projects, since they insure higher quality of product.

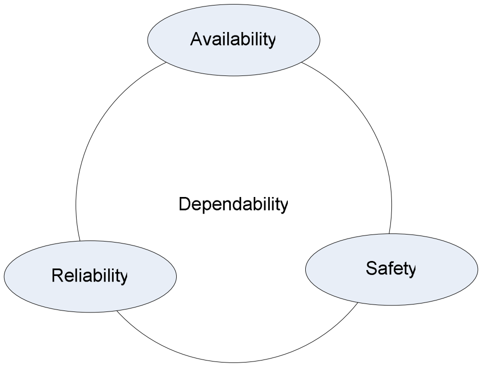


Figure 34 Focus of dependability

System complexity

Low cost demand and usability leads to integration of functional and safety systems. Increased complexity needs more controlled way of working and higher robustness of hardware. Especially specification becomes hard to handle with traditional tools. System design plays major role in reducing unnecessary complexity. Traditional sub-contracting should be replaced with partnership to enable efficient cross functional design teams. Setting up boundaries between design teams and relying solely to specifications tends to lead partial optimization. Separation of safety functions and other functions should be considered where possible without major decrease of usability.

For example basically all safety functions requiring other safe state than power OFF are really hard to design for vehicle environments, since there is normally only one battery system. Lead acid battery has failure rate of 30 / million miles according to Smith [1]. Say we assume that vehicle is operated 10 miles / hour speed, which is most probably too optimistic assumption. This leads to failure rate of 300 / million hour which is in the other words 3 * 10^{-4} / hours. When comparing to Table 1 one can figure out that rate is outside any safety integrity requirement. In most cases as simple as possible is best alternative!

Design work

Design process can be fine tuned endlessly, but there is no substitute for right engineering attitude. Design team must be motivated to work together to achieve true dependability in product. Sometimes biggest challenge in organization might be to maintain right safety attitude and being open towards new tools, since especially in the beginning they tend to take more time to use. Motivation should be done by showing the benefits from new work methods. After bad first impression most engineers tend to admit benefits from new tools and methods.

During concept design engineers are easily miss leaded to think only functionality. Special care should be paid on common parts in system which are not directly related to functions like power supplies. During the system design weakest links should be identified. It does not make sense to make chain stronger than weakest link, since in most cause it is costly. For example engineers tend to forget biggest failure cause, which is wiring and connectors in most systems.

Design work assessment should be more like coaching instead of audit in the end, because late changes due to assessment tend to be costly and complex. (Figure 35) Attention should be paid to on requirements management and specification phase. After concept phase assessor should be consulted to get first indications of success. After all true safety is built on right attitude from beginning of the project. Any audit process is not capable to supersede open minded and through engineering work.

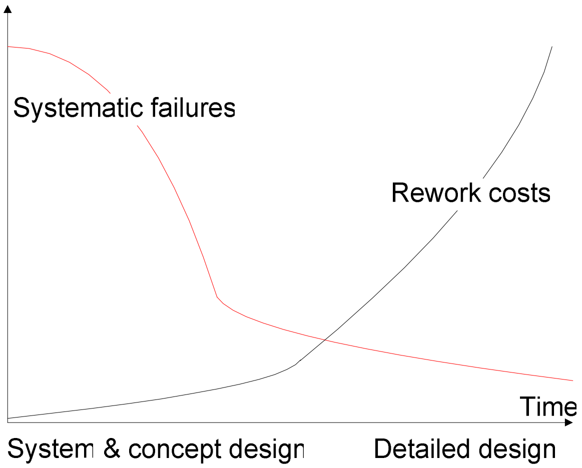


Figure 35 Failures created vs. rework costs [23]

Specification

Traceability seems to be most demanding challenge, when structural way of working is compared with traditional ways to make specifications. Specifications tools would help in process, but they do not make the work itself. They mainly help in traceability issues. Structured specification should be seen as an advantage. Well structured specification allows module level reuse of design. Good interface specifications makes concurrent engineering work easier and causes less rework.

Machinery control system

Appendix A checklist shows that project documentation is not finished and especially safe plan needs improvements. There is still lot of work to do on qualitative requirements before project can be accepted to safety usage. Table 21 summarizes quantitative requirements for machinery-control-system. Diagnostics and common cause points are under control, but overall failure rate needs small improvement.2815 FIT is in range compared to 1000 FIT and concept is anyway going to right direction. Figure 33 indicates that logic control part of the units should be improved, since it is a bottleneck in the design. Improved diagnostics could change dangerous undetected failures to detected failures or changes in circuitry could change failure modes to safe ones. For example using pull down instead of pull up or vice versa could lead to safe failure. In most cases simple changes in circuitry to change failure effect are more efficient than complex diagnostics. Quite often circuitry related directly to logic is dominated by microcontroller and they are inherently safe. Attention should be paid to glue logic and miscellaneous circuitry not related directly to functionality. For example intelligent power supply monitoring and sequencing could lower dangerous failures significantly.

Table 21Summary of machinery control system quantitative analysis

Discipline	Machinery concept result	SIL 2 level requirement
SFF consideration	96% (ECU)	>90%
Dangerous failure rate	2815 FIT	<1000 FIT
CCF consideration	75%	>65%

Future considerations

During this study work some notes were made what points could be improved in design flow. Work flow should follow more closely V-model. Present work flow is more water fall than V-model. Documentation model based on UML should be developed and structure of documentation reviewed even more deeply. Especially document change management needs attention. Work flow guidelines and recording of tasks should be more detailed. For example testing is often done, but evidence from the work is vague or not existing. Fault insertion testing is lacking from present work flow and strategy for it should be created.

From the technical point of view wireless communication will be very interesting in future, since absence of wiring have several benefits. Using wireless communication in critical systems has still many challenges to overcome. Many critical systems have electrically noisy environment and wireless security is far from wired system security.

Hints for efficient safety system design:

- Total cost instead of unit cost
- Concept phase work important
- Emphasize to start of project
- Requirements management
- Tracing between requirements and testing
- Weak links identified in system design
- Wiring and connectors
- Different technologies for redundancy
- Can system be designed to be inherently safe?
- Isolation of safety and non-safety
- Smart sensor interfacing
- Change management
- Burn in testing needed?
- Wear out limits for electronic units?
- Hardware category targeting could ease qualitative requirements
- All work should be documented carefully
- Keep it simple and motivate design team!

8. CONCLUSION

Need for highly dependable programmable machinery control system have become obvious during the last the decade. Traditionally machinery control systems have mechanical back up on control for critical functions, but modern systems rely solely to PE-systems also in critical functions. Recent development has been noticed by legal authorities and legislative requirements are effective soon for new products entering to market. Main focus in the study was to interpret standard requirements to process changes and to understand basic philosophy for reliable programmable system hardware. Usage of tools and methods were tested and demonstrated with machinery control system concept development.

Dependability should be seen as a product life cycle challenge. All steps of product life cycle from system analysis to decommissioning shall be planned and documented. Dependable control system provides continuously correct service for customer without hazardous consequences to people or public. System should be also maintained and modified in controlled manor. High dependability can be achieved trough careful and planned work during design, manufacturing and operation. Basic idea is avoidance of failures when possible, but all failures cannot be evaded. In case of failure system should react in controlled manner.

System analysis is focused to find links and chains between causes, failures and consequences. Discovered risks shall be quantified on their potentiality to harm people or environment. There is always a probability of catastrophic consequences, but likelihood should be on tolerable region compared to every day risks. OEM's set up goal for risk level reduction in final product and is responsible for risk analysis and validation of end product. Often contractors are responsible for realization phase of control system units. They should focus on fulfilling goal set by OEM. Good usage of proper tools provides evidence of work. Tools also guide work effort to right direction. FMEA analysis with fault tree diagrams provide good starting point for system and architecture level analysis. FMEDA provides evidence for final design integrity requirements.

Failures can be qualified to two groups. Firstly there are failures which occur randomly and consequences of those failures should be controlled and effects minimized. Quantitative requirements set a goal for random failure avoidance. Second failure category is systematic failures arising from wide range of causes. Quite often misunderstandings or lack of knowledge lead to specification mistakes. Mistakes during development are other primary cause for systematic failures. Qualitative requirements address systematic failures. In general avoidance of failures can be divided to four basic categories. Random failures should be controlled in proper manner. System should fail predictably and as planned. Hardware architecture selection should address single point failures and bottlenecks in system. Systematic error shall be avoided with proper work flow.

Random failures shall be addressed with adequate diagnostic coverage and fault tolerant circuit design. Component selection should emphasize reliability. Reliability oriented development process and proper work flow in every step of product lifecycle will lead to reduced number of systematic failures. V-model based development process is highly recommended to provide feedback between requirements and testing evidence. Structured work methods and specifications provide good traceability between requirements and testing. Misunderstandings can be minimized with unambiguous documents and work guidelines. Lot of effort should be paid to creation and verification of proper specification, since it reduces systematic errors and costs. Evidence of design correspondence to requirements should be demonstrated with testing on adequate level. Evidence of qualitative requirements is based on audits and documentations.

Typical system concept for machinery control is distributed system. Human interface device is located near operator and control unit is connected trough serial interface with it. CAN bus is widely used in automotive and industrial applications for communication between devices. Communication redundancy is needed and two separate CAN lines provide needed protection against wire breaks and communication errors. Communication is divided to two categories. Non-critical messaging uses only one dedicated CAN bus for system communication. Critical messages shall be transmitted in both CAN busses to achieve desired integrity level. Human interface device verifies that correct command is transmitted to system. Also intention of command is verified. ECU shall monitor system stage and operational conditions and makes decision to implement command only when it is safe.

Developed concept was analyzed starting from system level. Qualitative integrity level 2 was targeted. Analysis indicated that highest integrity requirement is Ag PL c. Level c can be implemented with several ways, but hardware category 2 was selected. Category 2 implementation can be used with integrity level 2 on AgPL c level design. Structured specification template was developed for use in Parker Vansco. Structure was needed to be able to fulfill tracking requirements. Fault tree method was introduced for block diagram level analysis. FMEDA design template was developed and failure rate data sources investigated. Siemens standard SN29500 was selected as a baseline failure rate data. Results from Fault tree and FMEDA analysis indicated that concept fulfills requirements quite well, but on detail level diagnostics should be improved especially on common parts.

Safety assessment analysis was implemented as much as possible on concept level to minimize large scale changes in the back end of the project. Safety assessment checklist was created for use in Parker Vansco. Lot of the safety related documentation must be created compared to projects with non-safe systems. Other general remark was that most of engineering tasks related to safety are done, but not documented thoroughly. Attention should be paid on creation of evidence from completed tasks. Electronic designs as such are already quite close to required level, because applications anyway call for high diagnostic coverage and reliability. Circuitry should be only fine tuned to achieve required integrity level.

Focus of dependability should be considered in the beginning of each project, since there is some trade offs between different dependability attributes. Focus can be either on absolute safety or in availability. Decisions should be based on legislative aspects and customer requirements. In general development of highly dependable systems is big challenge for organization from attitude point of view. There is no substitute for right attitude among engineers. From the technical point of view best alternatives are often the simplest ones!

REFERENCES

[1] Smith, David J., Simpson, Kenneth G. L. 2004. Functional safety. Second edition. Elsevier Ltd. 263 p.

[2] Smith, David J. 2005. Reliability, maintainability and risk. Seventh edition Elsevier Ltd. 346 p.

[3] Haikala, Ilkka, Märijärvi, Jukka 1998. Ohjelmistotuotanto. Viides painos. Suomen Atk-kustannus Oy. 385 p.

[4] Health and Safety Executive – UK. 2003.Out of Control: Why Control Systems go Wrong and How to Prevent Failure. Second edition.

[5] Jurgen, Ronald K. 2000. Automotive electronics reliability. Society of Automotive Engineers, Inc. 509 p.

[6] Avizienis, A. Laprie, J.C. Randell, B. *Fundamental Concepts of Dependability*. Research Report No 1145, LAAS-CNRS, April 2001

[7] Salo, Teemu. The art of developing embedded systems. Master of Science Thesis. December 2006. 53 p.

[8] IEC 61508, 2000, Functional safety of electrical/electronic/programmable electronic safety-related systems – 7 parts

[9] ISO/DIS 25119, Draft, 2008, Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems – 4 parts

[10] ISO/DIS 15998, 2008, Earth-moving machinery -- Machine-control systems (MCS) using electronic components -- Performance criteria and tests for functional safety

[11] DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery. 2006

[12] SN29500, 2008, Siemens Norm, Failure rates of components, 2008-02 Edition

[13] Weibull system analysis online reference 2007. Fault Tree Analysis and Reliability Block Diagrams [WWW]. [referenced 12.11.2009] Available: http://www.weibull.com/SystemRelWeb/blocksimtheory.htm

[14] UML standard [WWW]. [referenced 7.4.2009] Available: http://www.uml.org

[15] Wikipedia, Dependability. [WWW]. [referenced 12.11.2009] Available: http://en.wikipedia.org/wiki/Dependability

[16] Wikipedia, Failure mode bathtub curve [WWW]. [referenced 12.11.2009] Available: http://en.wikipedia.org/wiki/File:Bathtub_curve.jpg

[17] Intersil HIP9010 knock detection IC datasheet [WWW]. [referenced 7.4.2009] Available: http://www.intersil.com/data/fn/fn3601.pdf

[18] TI TMP101 I2C temperature sensor IC datasheet [WWW]. [referenced 7.4.2009] Available: http://focus.ti.com/lit/ds/symlink/tmp101.pdf

[19] ISO 11898-1:2003, Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signaling. 2003

[20] Official journal of European Union -- Commission communication in the framework of the implementation of the Directive 2006/42/EC of the European Parliament and of the Council on machinery, and amending Directive 95/16/EC. 29.12.2009.

[21] Pat. FI 20075366. INDICATOR ARRANGEMENT Wärtsilä finland Oy, Vaasa. (SAIKKONEN ARI [FI]; LAAKSO PERRI [FI]; KALLIO MARKKU [FI]; SALOJAERVI ANTERO [FI]).
Hak.nro FI20070005366 20070521. 19 p.

[22] Forsman, Tommi. Luoma, Tomi. Salojärvi, Antero. DPA functional requirements specification, First draft. Vansco Electronics Oy. Parker Vansco internal confidential document. 8.12.2009. 16 p.

[23] Repo, Jorma. Pirel projektipäälikkökoulutus / Projektien ohjaus ja hallinta. Edutech. 22.10.2002. 37 p.

APPENDIX A

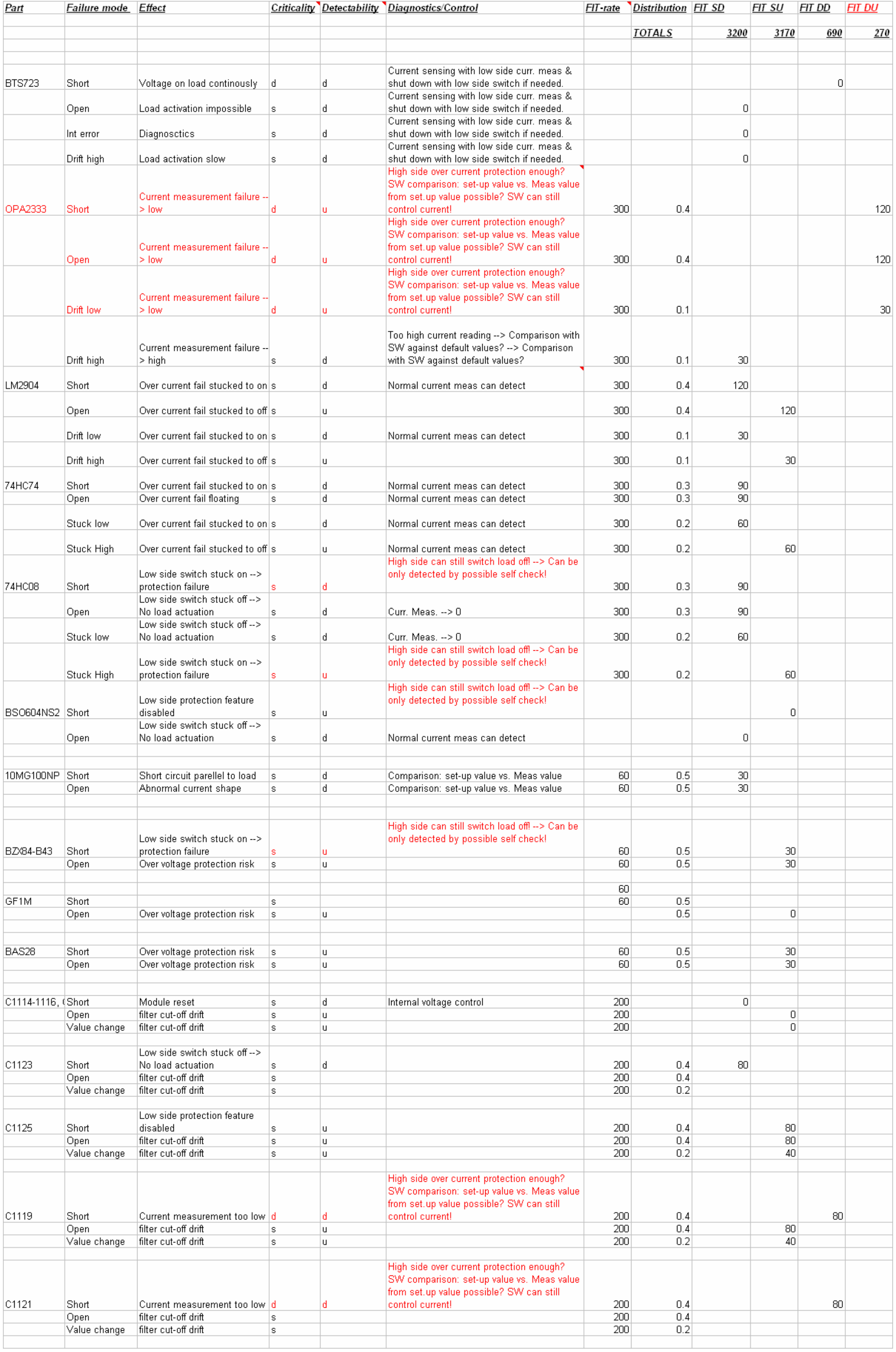
Safety assessment checklist for machinery control concept project at present status

Requirement	Evidence	OK
General		
Quality plan	Vansco Electronics QS	OK
Safety plan		
Documentation plan		
Project management (According to company QS)	Vansco Electronics QS	OK
Life cycle		
Product life cycle plan (According to company QS including modifications and failure logging)	Vansco Electronics QS	OK
Product life cycle audit		
Specification		
Unambiguous	Review minutes	OK
Structured	Review minutes	OK
Safety function description with Integrity requirement	Review minutes	OK
Operational modes	Review minutes	OK
Safety / non-safety isolation	Review minutes	OK
Specification inspection	Review minutes	OK
Design and development		
Design guides	Vansco Electronics QS	OK
Design standards	Vansco Electronics QS	OK
Design documentation	Vansco Electronics QS	OK??
Structured design		
Use of proven designs		
Modular design		
Reliability margining		
Safe failure modes		
Failure detection methods		
Communication errors		
Change of safety related HW and SW prohibited from user		
User interface design		
Fault tolerance techniques		
Environmental stress screening		
Failure mode testing		
Quantitative requirements		
Safe failure fraction demonstration (FMEDA)		
Random failure demonstration (FMEDA)		
Common cause estimates		
Testing and integration		
Test plan (acceptance criteria, tools and set up)		

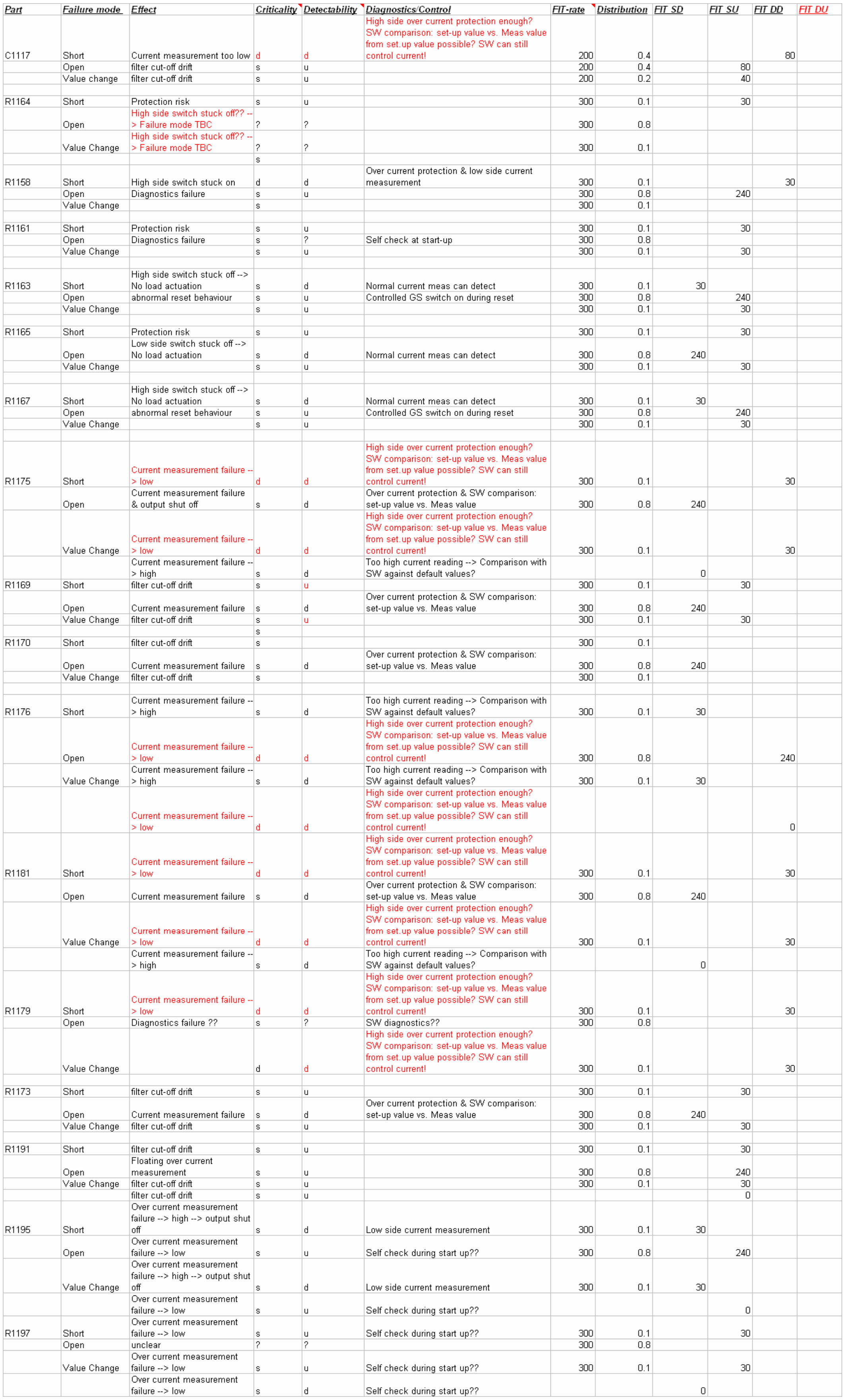
Functional testing (cross referencing and out boundaries testing)		
Component environmental tests		
Component interference tests		
Component fault insertion testing		
Test log audit		
Operations and maintenance		
Preventive maintenance		
Proof testing schedule		
Pilot installation audit		
Failure logging		
Operator friendliness		
Restricted operator access		
Operator training		
Purchasing		
Supplier audits	Vansco Electronics QS	OK
Validation		
Validation plan		
System functional tests		
System environmental tests		
System interference tests		
System fault insertion testing		
Safety functionality during faulty operating conditions		
Validation log audit		

APPENDIX B

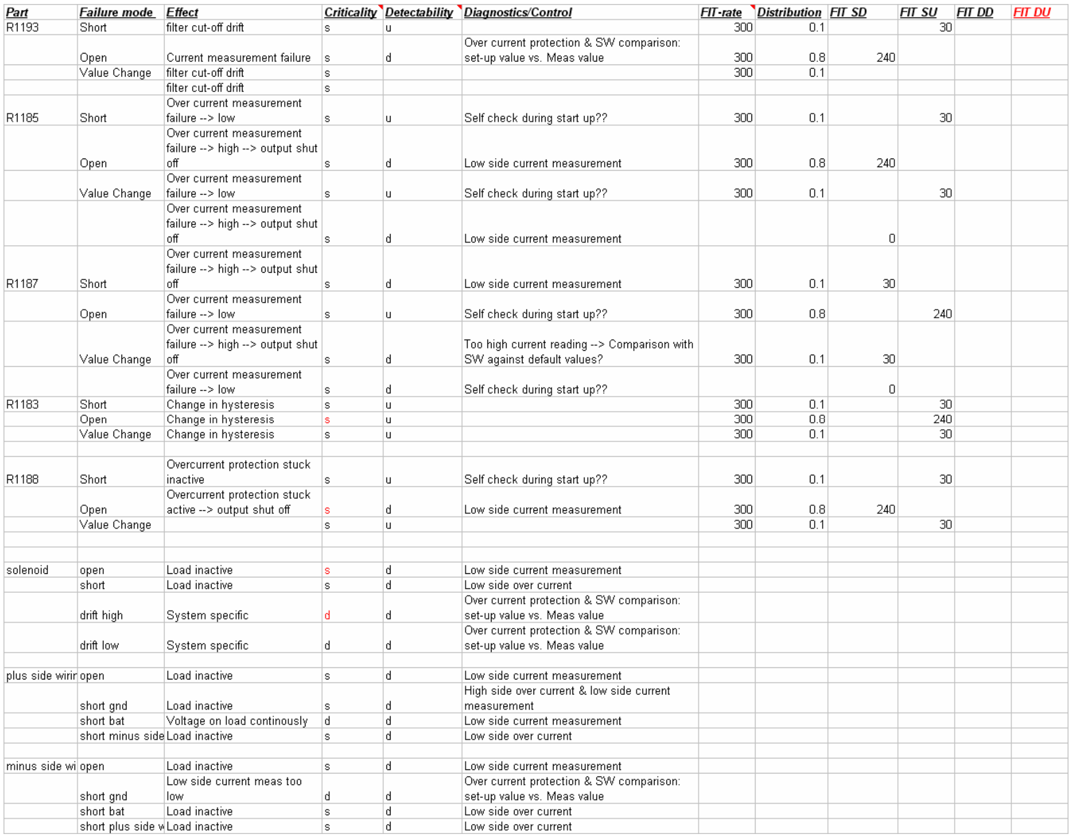
FMEDA calculation sheet for solenoid driver block



Part	*Failure mode*	*Effect*	*Criticality*	*Detectability*	*Diagnostics/Control*	*FIT-rate*	*Distribution*	*FIT SD*	*FIT SU*	*FIT DD*	*FIT DU*
							TOTALS	*3200*	*3170*	*690*	*270*
BTS723	Short	Voltage on load continously	d	d	Current sensing with low side curr. meas & shut down with low side switch if needed.					0	
	Open	Load activation impossible	s	d	Current sensing with low side curr. meas & shut down with low side switch if needed.			0			
	Int error	Diagnosctics	s	d	Current sensing with low side curr. meas & shut down with low side switch if needed.			0			
	Drift high	Load activation slow	s	d	Current sensing with low side curr. meas & shut down with low side switch if needed.			0			
OPA2333	Short	Current measurement failure --> low	d	u	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.4				120
	Open	Current measurement failure --> low	d	u	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.4				120
	Drift low	Current measurement failure --> low	d	u	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1				30
	Drift high	Current measurement failure --> high	s	d	Too high current reading --> Comparison with SW against default values? --> Comparison with SW against default values?	300	0.1	30			
LM2904	Short	Over current fail stucked to on	s	d	Normal current meas can detect	300	0.4	120			
	Open	Over current fail stucked to off	s	u		300	0.4		120		
	Drift low	Over current fail stucked to on	s	d	Normal current meas can detect	300	0.1	30			
	Drift high	Over current fail stucked to off	s	u		300	0.1		30		
74HC74	Short	Over current fail stucked to on	s	d	Normal current meas can detect	300	0.3	90			
	Open	Over current fail floating	s	d	Normal current meas can detect	300	0.3	90			
	Stuck low	Over current fail stucked to on	s	d	Normal current meas can detect	300	0.2	60			
	Stuck High	Over current fail stucked to off	s	u	Normal current meas can detect	300	0.2		60		
74HC08	Short	Low side switch stuck on --> protection failure	s	d	High side can still switch load off! --> Can be only detected by possible self check!	300	0.3	90			
	Open	Low side switch stuck off --> No load actuation	s	d	Curr. Meas. --> 0	300	0.3	90			
	Stuck low	Low side switch stuck off --> No load actuation	s	d	Curr. Meas. --> 0	300	0.2	60			
	Stuck High	Low side switch stuck on --> protection failure	s	u	High side can still switch load off! --> Can be only detected by possible self check!	300	0.2		60		
BSO604NS2	Short	Low side protection feature disabled	s	u	High side can still switch load off! --> Can be only detected by possible self check!				0		
	Open	Low side switch stuck off --> No load actuation	s	d	Normal current meas can detect			0			
10MG100NP	Short	Short circuit parellel to load	s	d	Comparison: set-up value vs. Meas value	60	0.5	30			
	Open	Abnormal current shape	s	d	Comparison: set-up value vs. Meas value	60	0.5	30			
BZX84-B43	Short	Low side switch stuck on --> protection failure	s	u	High side can still switch load off! --> Can be only detected by possible self check!	60	0.5		30		
	Open	Over voltage protection risk	s	u		60	0.5		30		
						60					
GF1M	Short		s			60	0.5				
	Open	Over voltage protection risk	s	u			0.5		0		
BAS28	Short	Over voltage protection risk	s	u		60	0.5		30		
	Open	Over voltage protection risk	s	u		60	0.5		30		
C1114-1116, (	Short	Module reset	s	d	Internal voltage control	200		0			
	Open	filter cut-off drift	s	u		200			0		
	Value change	filter cut-off drift	s	u		200			0		
C1123	Short	Low side switch stuck off --> No load actuation	s	d		200	0.4	80			
	Open	filter cut-off drift	s			200	0.4				
	Value change	filter cut-off drift	s			200	0.2				
C1125	Short	Low side protection feature disabled	s	u		200	0.4		80		
	Open	filter cut-off drift	s	u		200	0.4		80		
	Value change	filter cut-off drift	s	u		200	0.2		40		
C1119	Short	Current measurement too low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	200	0.4			80	
	Open	filter cut-off drift	s	u		200	0.4		80		
	Value change	filter cut-off drift	s	u		200	0.2		40		
C1121	Short	Current measurement too low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	200	0.4			80	
	Open	filter cut-off drift	s			200	0.4				
	Value change	filter cut-off drift	s			200	0.2				



Part	Failure mode	Effect	Criticality	Detectability	Diagnostics/Control	FIT-rate	Distribution	FIT SD	FIT SU	FIT DD	FIT DU
C1117	Short	Current measurement too low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	200	0.4			80	
	Open	filter cut-off drift	s	u		200	0.4		80		
	Value change	filter cut-off drift	s	u		200	0.2		40		
R1164	Short	Protection risk	s	u		300	0.1		30		
	Open	High side switch stuck off?? --> Failure mode TBC	?	?		300	0.8				
	Value Change	High side switch stuck off?? --> Failure mode TBC	?	?		300	0.1				
			s								
R1158	Short	High side switch stuck on	d	d	Over current protection & low side current measurement	300	0.1			30	
	Open	Diagnostics failure	s	u		300	0.8		240		
	Value Change		s			300	0.1				
R1161	Short	Protection risk	s	u		300	0.1		30		
	Open	Diagnostics failure	s	?	Self check at start-up	300	0.8				
	Value Change		s	u		300	0.1		30		
R1163	Short	High side switch stuck off --> No load actuation	s	d	Normal current meas can detect	300	0.1	30			
	Open	abnormal reset behaviour	s	u	Controlled GS switch on during reset	300	0.8		240		
	Value Change		s	u		300	0.1		30		
R1165	Short	Protection risk	s	u		300	0.1		30		
	Open	Low side switch stuck off --> No load actuation	s	d	Normal current meas can detect	300	0.8	240			
	Value Change		s	u		300	0.1		30		
R1167	Short	High side switch stuck off --> No load actuation	s	d	Normal current meas can detect	300	0.1	30			
	Open	abnormal reset behaviour	s	u	Controlled GS switch on during reset	300	0.8		240		
	Value Change		s	u		300	0.1		30		
R1175	Short	Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1			30	
	Open	Current measurement failure & output shut off	s	d	Over current protection & SW comparison: set-up value vs. Meas value	300	0.8	240			
	Value Change	Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1			30	
		Current measurement failure --> high	s	d	Too high current reading --> Comparison with SW against default values?			0			
R1169	Short	filter cut-off drift	s	u		300	0.1		30		
	Open	Current measurement failure	s	d	Over current protection & SW comparison: set-up value vs. Meas value	300	0.8	240			
	Value Change	filter cut-off drift	s	u		300	0.1		30		
			s								
R1170	Short	filter cut-off drift	s			300	0.1				
	Open	Current measurement failure	s	d	Over current protection & SW comparison: set-up value vs. Meas value	300	0.8	240			
	Value Change	filter cut-off drift	s			300	0.1				
R1176	Short	Current measurement failure --> high	s	d	Too high current reading --> Comparison with SW against default values?	300	0.1	30			
	Open	Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.8			240	
	Value Change	Current measurement failure --> high	s	d	Too high current reading --> Comparison with SW against default values?	300	0.1	30			
		Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!					0	
R1181	Short	Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1			30	
	Open	Current measurement failure	s	d	Over current protection & SW comparison: set-up value vs. Meas value	300	0.8	240			
	Value Change	Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1			30	
		Current measurement failure --> high	s	d	Too high current reading --> Comparison with SW against default values?			0			
R1179	Short	Current measurement failure --> low	d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1			30	
	Open	Diagnostics failure ??	s	?	SW diagnostics??	300	0.8				
	Value Change		d	d	High side over current protection enough? SW comparison: set-up value vs. Meas value from set.up value possible? SW can still control current!	300	0.1			30	
R1173	Short	filter cut-off drift	s	u		300	0.1		30		
	Open	Current measurement failure	s	d	Over current protection & SW comparison: set-up value vs. Meas value	300	0.8	240			
	Value Change	filter cut-off drift	s	u		300	0.1		30		
R1191	Short	filter cut-off drift	s	u		300	0.1		30		
	Open	Floating over current measurement	s	u		300	0.8		240		
	Value Change	filter cut-off drift	s	u		300	0.1		30		
		filter cut-off drift	s	u					0		
R1195	Short	Over current measurement failure --> high --> output shut off	s	d	Low side current measurement	300	0.1	30			
	Open	Over current measurement failure --> low	s	u	Self check during start up??	300	0.8		240		
	Value Change	Over current measurement failure --> high --> output shut off	s	d	Low side current measurement	300	0.1	30			
		Over current measurement failure --> low	s	u	Self check during start up??				0		
R1197	Short	Over current measurement failure --> low	s	u	Self check during start up??	300	0.1		30		
	Open	unclear	?	?		300	0.8				
	Value Change	Over current measurement failure --> low	s	u	Self check during start up??	300	0.1		30		
		Over current measurement failure --> low	s	d	Self check during start up??			0			



Part	***Failure mode***	***Effect***	***Criticality***	***Detectability***	***Diagnostics/Control***	***FIT-rate***	***Distribution***	***FIT SD***	***FIT SU***	***FIT DD***	***FIT DU***
R1193	Short	filter cut-off drift	s	u		300	0.1		30		
	Open	Current measurement failure	s	d	Over current protection & SW comparison: set-up value vs. Meas value	300	0.8	240			
	Value Change	filter cut-off drift	s			300	0.1				
		filter cut-off drift	s								
R1185	Short	Over current measurement failure --> low	s	u	Self check during start up??	300	0.1		30		
	Open	Over current measurement failure --> high --> output shut off	s	d	Low side current measurement	300	0.8	240			
	Value Change	Over current measurement failure --> low	s	u	Self check during start up??	300	0.1		30		
		Over current measurement failure --> high --> output shut off	s	d	Low side current measurement			0			
R1187	Short	Over current measurement failure --> high --> output shut off	s	d	Low side current measurement	300	0.1	30			
	Open	Over current measurement failure --> low	s	u	Self check during start up??	300	0.8		240		
	Value Change	Over current measurement failure --> high --> output shut off	s	d	Too high current reading --> Comparison with SW against default values?	300	0.1	30			
		Over current measurement failure --> low	s	d	Self check during start up??			0			
R1183	Short	Change in hysteresis	s	u		300	0.1		30		
	Open	Change in hysteresis	s	u		300	0.8		240		
	Value Change	Change in hysteresis	s	u		300	0.1		30		
R1188	Short	Overcurrent protection stuck inactive	s	u	Self check during start up??	300	0.1		30		
	Open	Overcurrent protection stuck active --> output shut off	s	d	Low side current measurement	300	0.8	240			
	Value Change		s	u		300	0.1		30		
solenoid	open	Load inactive	s	d	Low side current measurement						
	short	Load inactive	s	d	Low side over current						
	drift high	System specific	d	d	Over current protection & SW comparison: set-up value vs. Meas value						
	drift low	System specific	d	d	Over current protection & SW comparison: set-up value vs. Meas value						
plus side wirir	open	Load inactive	s	d	Low side current measurement						
	short gnd	Load inactive	s	d	High side over current & low side current measurement						
	short bat	Voltage on load continously	d	d	Low side current measurement						
	short minus side	Load inactive	s	d	Low side over current						
minus side wi	open	Load inactive	s	d	Low side current measurement						
	short gnd	Low side current meas too low	d	d	Over current protection & SW comparison: set-up value vs. Meas value						
	short bat	Load inactive	s	d	Low side over current						
	short plus side w	Load inactive	s	d	Low side over current						